CYNTHIA R. COOK, DAVID LUCKEY, BRADLEY KNOPP,
YULIYA SHOKH, KAREN M. SUDKAMP, DON CASLER,
YOUSUF ABDELFATAH, HILARY REININGER

Improving Intelligence Support to the Future Warfighter

Acquisition for the Contested Environment

For more information on this publication, visit **www.rand.org/t/RRA537-1**.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0814-3

Cover: oonal/Getty images.

Limited Print and Electronic Distribution Rights

Preface

The United States faces new and increasingly sophisticated threats from peer and near-peer adversaries. The 2018 National Defense Strategy (NDS) describes an "increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations." General Charles Q. Brown argues that in response the Air Force needs to accelerate its improvements to meet and, to the extent possible, counter these threats or risk losing the next major war. That necessitates having an acquisition system that is postured to produce the weapon systems that can "fly, fight and win" against capable adversaries. This report addresses the challenge of threat informed acquisition in a contested environment and offers recommendations to increase the efficiency and effectiveness of Air Force intelligence support to the acquisition community to improve existing and future acquisition strategies and programs.

The research reported here was commissioned by the Air Force Material Command (AFMC)/Intelligence Directorate (A2) and conducted within the Resource Management Program of RAND Project AIR FORCE as part of a fiscal year 2020 project Threat-Informed Acquisition Strategy and Decisionmaking for the Contested Environment.

The RAND Corporation is committed to ethical and respectful treatment of RAND research participants and complies with all applicable laws and regulations, including the *Federal Policy for the Protection of Human Subjects*, also known as the "Common Rule." The research described in this report was screened and, if necessary, reviewed by

RAND's Human Subjects Protection Committee, which serves as RAND's institutional review board (IRB) charged with ensuring the ethical treatment of individuals who are participants in RAND projects through observation, intervention, interaction, or use of data about them. RAND's Federalwide Assurance (FWA) for the Protection of Human Subjects (FWA00003425, effective until June 22, 2023) serves as our assurance of compliance with federal regulations.

The views of any unnamed sources are solely their own and do not represent the official policy or position of any department or agency of the U.S. government.

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Workforce, Development, and Health; and Resource Management. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website: www.rand.org/paf/

This report documents work originally shared with the DAF on September 18, 2020. The draft report, issued on September 30, 2020, was reviewed by formal peer reviewers and DAF subject-matter experts.

Contents

Figures and Tables

Figures

Tables

Summary

Issue

Unlike in the preceding two decades of combat operations in the Middle East, the United States now faces new and increasingly sophisticated threats from peer and near-peer adversaries. The 2018 National Defense Strategy (NDS) describes an "increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations."[1] The Chief of Staff of the Air Force (CSAF) has argued that in response the Air Force needs to accelerate its improvements to meet and, to the extent possible, counter these threats or risk losing the next major war. That necessitates having an acquisition system that is postured to produce the weapon systems that can "fly, fight and win" against capable adversaries that pose a threat, both currently and in the future.

Approach

To address these challenges to the acquisition system, we divided the research into four tasks: (1) reviewing and analyzing relevant background material, (2) investigating the current Air Force process for intelligence support for acquisition, (3) evaluating current processes to

[1] DoD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018a, p. 2.

find appropriate connections between intelligence and acquisition, and (4) documenting the research results, including making recommendations for improvement.

Conclusions

We found that ensuring the ability of the Air Force acquisition community to deliver capabilities—especially ones that meet a threat as it exists when capabilities are delivered, not as it was when requirements were set—is a complex and complicated challenge. It requires understanding the distinct cultures, goals, resource restraints and constraints, and incentives of the acquisition and intelligence enterprises themselves—characteristics that have been shaped in the decades when the U.S. military was globally dominant, and its weaponry had no peer. It also requires an understanding of the connection between these acquisition and intelligence enterprises. At the same time, it requires an understanding of the larger environment in which these enterprises operate, which includes the Department of Defense (DoD) and the U.S. Intelligence Community (IC) as well as Congress and other stakeholders, all of whom serve as resources and impose additional restraints and constraints on the "acquisition intelligence enterprise ecosystem."

We have identified issues that are complicated and complex, but not impossible to resolve. Optimal resolution requires a concerted effort across many domains, in various systems and subsystems, across two enterprises, and over an extended period. For example, informal communication channels are an important part of the intelligence support to acquisition process, above and beyond the formal requirements, and this information exchange should be understood and encouraged. Although this could lead to inefficiencies and lack of prioritization, which in turn could result in uneven information distribution across programs since intelligence information produced under informal request might not be available to other potential users and result in possible duplication of effort or, worse, duplication of questions that result in different answers, there are mitigations to these risks.

There are many aspects to this challenge confronting the Air Force in its quest to incorporate intelligence to the extent necessary and possible into its acquisition efforts. To be clear, there is no single, simple answer to this problem. In fact, there is no answer that will fully resolve this problem. There are, however, many things that can be done to resolve various aspects of this problem that, when taken together, will improve Air Force acquisition efforts by including more and better quality (more focused) intelligence. There is also a temporal aspect to this challenge like other intelligence issues. There is no such thing as perfect intelligence; there is no crystal ball. Additionally, the best intelligence possible provided too late in the acquisition cycle provides less than the best value, and possibly little value at all. Our goal in this report is to reflect on the challenge and offer recommendations for improvement. That said, readers may see specific examples that don't align with their own experiences. It is difficult to capture the entire range of experiences in a summary report, so we ask the reader to keep in mind the larger intent of the report, which is to provide recommendations for the Air Force to consider improving the value that intelligence can and must provide to Air Force acquisition efforts.

Recommendations

- The intelligence support to the acquisition enterprise ecosystem is comprised of several entities. These entities have no single, common chain of command, and they connect via both structured (formal) and unstructured (informal) mechanisms. This connection requires support from U.S. Air Force senior leadership both to ensure change across the enterprise and to advocate for change for assets controlled outside of the Air Force. Additionally, senior leadership across all Air Force elements should continue to stress the importance of incorporating threat information into acquisition—and to make resources available for doing so. Intelligence support is not free.
- Acquisition policy and guidance do not always clarify and reinforce how and when intelligence can be continuously integrated

into the acquisition process (not just at formal acquisition milestones). Emphasis is placed on cost, schedule, and performance as assigned from the requirements and budgetary communities. Thus, the requirements and budgetary community must be partners with acquisition in seeking and digesting intelligence and continually assessing and trading resources to address the biggest evolving threats. Similarly, and in accordance with institutional guidance, intelligence focuses on offering near-term (and possibly urgent) tactical and operational support and strategic intelligence support to the warfighter and policymaker, due to their time-sensitivity, before supporting other needs, such as acquisition. Updating policy and guidance (and ensuring adequacy of resources) can help to ensure that sufficient attention is paid to acquisitions. Continually relegating intelligence support to acquisition after support to the warfighter and policymaker places the future warfighter at greater risk.

- Incentive structures are not in alignment with the goal of threat-informed acquisition, but could be improved if acquisition metrics are changed. For example, programs could be measured against updated baselines instead of original baselines, when threats are addressed midcourse. Also, programs could be measured explicitly on how well they address flexibility in the form of open systems architectures and better mechanisms to seek additional investments. Changing these metrics can change the demand signal.
- Formal methods of communicating threat and ensuring that programs are threat-informed, such as threat steering groups (TSGs), threat working groups (TWGs), validated online life-cycle threat (VOLTs), and critical intelligence parameters (CIPs), are useful, but do not always get the attention of busy program management. Additional intelligence support at program executive officers (PEOs) and program offices is needed and could provide needed assistance.
- Outdated and inadequate information technology (IT) infrastructure, which creates challenges and limits to information access, can be addressed with additional investments, some of which may

need to be borne in acquisition program budgets. The U.S. Air Force does not control and thus would need to advocate for change for infrastructure controlled outside the U.S. Air Force, such as the Community On-Line Intelligence System for End Users (COLISEUM), which is managed by the Defense Intelligence Agency (DIA).

- Limits on clearances within the acquisition community reduce comprehension of the true nature of the threat and thus the urgency of the response. On the intelligence side, limits on access to special access program (SAP) information by the IC create support challenges. This could be addressed by improving access availability or by seeking ways to extract less-classified insight from higher-classification documents for wider dissemination and investing in improving appropriate clearances. Lack of information on either side of the intelligence-acquisition equation limits the objectives of both.
- The intelligence workforce supporting acquisition (the "acquisition intelligence" workforce) is likely understaffed in several areas, and many analysts lack the proper skills. This can be addressed by improving hiring, training, and retention practices, and efforts are currently underway to address some of these issues (e.g., the creation of the Acquisition Intelligence Career Occupation Program Foundational Credential, the creation of an Individual Capability Management [ICM] code, and the PALACE ACQUIRE [PACQ] program). We suggest these efforts, and others like them, continue. In the end, progress is driven by people. The Air Force requires the best available.

We note that some of these recommendations will simply require more resources to be provided to intel support to acquisition. Others may require a reprioritization—prioritizing acquisition higher as it competes for intel resources or prioritizing intel inputs higher as it competes with cost, schedule, and performance in the acquisition process. And those additional resources or changed priorities can only come from senior DAF leadership. We make recommendations about the mechanisms to accomplish change—Policy, Metrics, Communication and IT,

et cetera—but those mechanisms have to be underwritten by resources, an ever-present challenge in effective change management.

Acknowledgments

The RAND Project AIR FORCE (PAF) project team would like to thank Colonel Frank Schreiber, USAF, Dr. Daniel Atkins, and the staff of the U.S. Air Force Materiel Command and other U.S. Air Force staff for their support and assistance during this project. At least 75 individuals inside and outside the Department of the Air Force gave their time and offered their insights for this effort across the acquisition, intelligence, and requirements communities. All participants spoke on a nonattribution basis, and although we cannot mention them by name, we are grateful for their inputs. Special thanks go to Captain Ron Zimmerman, Jonathon "Rusty" May, Kelly Altic, and others in the sponsor office for their ongoing support.

We would also like to thank our RAND colleague Gordon Lee for communications analysis expertise that helped to shape and clarify our message. We thank Obaid Younossi, Stephanie Young, Patrick Mills, and Anu Narayanan for Resource Management Program leadership and management; and Ted Harshberger for PAF leadership. Jim Williams offered useful comments on an earlier draft. Finally, we are grateful to our peer reviewers, Philip Antón and Jonathan Wong, for their exceptional thoughtful and careful expert reviews, which substantially improved both the quality and readability of this report.

While we are thankful for the assistance provided by those listed above and others, we ask that you attribute any errors or omissions solely to the authors.

Abbreviations

A2	Intelligence Directorate
ACAT	acquisition category
ACC	Air Combat Command
AD	active duty
AEDC	Arnold Engineering and Development Center
AFB	Air Force base
AFCEC	Air Force Civil Engineering Center
AF/A2/6	DAF Intelligence, Surveillance, Reconnaissance and Cyber Effects
AF/A5/8	DAF Strategic Plans and Requirements
AFI	Air Force Instruction
AFIMSC	Air Force Installation and Mission Support Center
AFISRA	Air Force Intelligence, Surveillance, and Reconnaissance Agency
AFIT	Air Force Institute of Technology
AFLCMC	Air Force Life-Cycle Management Center
AFMAN	Air Force Manual
AFMC	Air Force Materiel Command
AFNWC	Air Force Nuclear Weapons Center
AFOSI	Air Force Office of Special Investigations
AFOTEC	Air Force Operational Test and Evaluation Center
AFPC	Air Force Personnel Center

AFPEO	Air Force Program Executive Office
AFR	Air Force Reserve
AFRID	Air Force Requirements Integration Division
AFRL	Air Force Research Laboratory
AFROC	Air Force Requirements Oversight Council
AFRRG	Air Force Requirements Review Group
AFSC	Air Force Specialty Code
AFSPC	Air Force Space Command
AFTC	Air Force Test Center
AFWIC	Air Force Weapons Integration Center
AIEET	Acquisition and Intelligence Experience Exchange Tour
AMC	Air Mobility Command
ANG	Air National Guard
AoA	analysis of alternatives
AOR	area of operations
APB	Acquisition Program Baseline
AT&L	Acquisitions, Technology, and Logistics
C3I&N	command, control, communications, intelligence and networks
CCMD	combatant command
CDD	capability development document
CENTCOM	central command
CFM	career field manager
CI	counterintelligence
CIP	critical intelligence parameter
COLISEUM	Community On-Line Intelligence System for End Users and Managers
CPI	critical program information
CSAF	Chief of Staff of the Air Force

DAF	Department of the Air Force
DAS	Defense Acquisition System
DAU	Defense Acquisition University
DIA	Defense Intelligence Agency
DIAI	Defense Intelligence Agency Instruction
DIAP	Defense Intelligence Analysis Program
DIE	Defense Intelligence Enterprise
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoI	Director of Intelligence
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
DT&E	developmental testing and evaluation
ED	engineering degree
EWI	education with industry
FAR	Federal Acquisition Regulations
FIE	foreign intelligence entity
FY	fiscal year
GAO	Government Accountability Office
GEOINT	Geospatial Intelligence
HAF	Headquarters Air Force
IC	U.S. Intelligence Community
ICD	initial capability document
ICM	individual capability management
IFTU	Intelligence Formal Training Unit
IMD	intelligence mission data
IMDC	Intelligence Mission Data Center
IMS	installations and mission support

IN	Intelligence Directorate
IPC	Intelligence Production Center
IS	intelligence squadron
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council
JWICS	Joint Worldwide Intelligence Communication System
LCSP	life-cycle sustainment plan
M&S	modeling and simulation
MDA	milestone decision authority
MDAP	Major Defense Acquisition Program
MDD	materiel development decision
MIE	materiel intelligence enterprise
MilPDS	Military Personnel Database System
MOU	memorandum of understanding
MSA	materiel solution analysis
NASIC	National Air and Space Intelligence Center
NDS	National Defense Strategy
NGA	National Geospatial-Intelligence Agency
NSA	National Security Agency
OPEX	operational experience
OPR	office of primary responsibility
OT&E	operational testing and evaluation
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PACQ	PALACE ACQUIRE
PAF	Project AIR FORCE

PEO	program executive office
PIR	priority intelligence requirement
PM	program manager
PoA	program of analysis
PPBE	planning, programming, budgeting and execution, and evaluation
PPP	program protection plan
RCO	Rapid Capabilities Office
RDT&E	Research, development, test and evaluation
RFI	request for information
S&TI	Scientific and technical intelligence
SAF/AQ	Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics
S/E/A	scientists, engineers, and acquisition
SAP	special access program
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SCRM	supply-chain risk management
SEI	special experience identifier
SIPRnet	Secure Internet Protocol Router Network
SMC	Space and Missile Systems Center
SME	subject-matter expert
T&E	testing and evaluation
TL	threat library
TLA	technology and long-range analysis
TMMR	technology maturation and risk reduction
TS	top secret
TSG	threat steering group
TTRA	technology targeting risk assessment
TW	test wing

TWG	threat working group
USAF	United States Air Force
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I&S)	Under Secretary of Defense for Intelligence and Security
VOLT	validated online life-cycle threat
WPAFB	Wright Patterson Air Force Base

CHAPTER ONE

Introduction

The Strategic Challenge

The United States faces new and increasingly sophisticated threats from peer and near-peer adversaries, in contrast to the opponents it faced in the field in the two decades after September 11. The 2018 National Defense Strategy (NDS) describes an "increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations."[1] China and Russia are highlighted as the sources of this threat.

This represents a change from the engagements in which the United States has participated since September 11, 2001, when the U.S. military had a decisive advantage, including larger stockpiles and more capable weapon systems than our adversaries in Afghanistan and Iraq. In 2017, Marine Corps General Joseph F. Dunford, Jr., who was Chairman of the Joint Chiefs of Staff, stated to the Senate Appropriations Committee Defense Subcommittee, "In just a few years, if we do not change our trajectory, we will lose our qualitative and quantitative competitive advantage."[2]

---

[1] DoD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018a.

[2] Jim Garamone, "Mattis: 2018 Budget Will Continue Readiness Recovery," U.S. Army, June 15, 2017.

Still more recently, the Chief of Staff of the U.S. Air Force (CSAF), General Charles Q. Brown, highlighted the necessity of preparing to meet more capable adversaries. In his August 2020 strategic approach, "Accelerate Change or Lose," General Brown argued that the U.S. Air Force (USAF) "must adapt and accelerate—now—to ensure our continued ability to best serve our Nation."[3]

Part of ensuring that USAF and other U.S. military branches are postured to meet the threat is ensuring that the materiel capabilities—the weapon systems—upon which they rely can compete effectively against current and emergent capabilities possessed by adversaries. CSAF's message bluntly argues that the United States risks an erosion in its warfighting advantage. While the U.S. military focused on counterinsurgency operations against violent extremists in the central command (CENTCOM) area of operations (AOR) for the last two decades, the message notes that "our competitors [especially China] focused on defeating us. They have studied, resourced, and introduced systems specifically designed to defeat the USAF capabilities that have underpinned the American way of war for a generation."[4] At the same time, the last 20 years of operations focused in the CENTCOM AOR has taken a toll on the force and the equipment, even as U.S. technological advantages there meant less pressure from the requirements community to focus the acquisition system on the near-peer threat.

CSAF Brown's vision offers a strategic approach to acquisition that reflects this recognition:

> We must design our capabilities and concepts to defeat our adversaries, exploit their vulnerabilities, and play to our strengths. And we must be able to frame decisions and trade-offs with both a near and long-term view of what value our capabilities provide throughout the lifecycle of performance.
>
> To do this, we must reframe platform-centric debates to focus instead on capabilities to execute the mission relative to our adversaries. Programs that once held promise, but are no longer

[3] Charles Q. Brown, Jr., "Accelerate Change or Lose," *Air Force Magazine*, August 2020, p. 4.

[4] Brown, 2020, p. 3.

> affordable or will not deliver needed capabilities on competition-relevant timelines, must be divested or terminated. Cost, schedule, and performance metrics alone are no longer sufficient metrics of acquisition success. We must be able to account for the interactive nature of competition and continuously assess ourselves relative to our adversaries' adaptations.[5]

CSAF's vision argues that capability requirements must clearly be determined by the threat. Acquisition programs, however, must also continually consider the evolving threat over their lifespans. U.S. adversaries are threatening the nation's air superiority across systems' survivability and offensive capabilities. Any strategic defensive responses need to recognize the capability life cycle of U.S. systems to engage reactively with what the adversaries are doing and to evolve programs to ensure their continued effectiveness.

This message is repeated elsewhere in the U.S. Air Force. In the Air Force Materiel Command (AFMC) Strategic Plan, released in July 2020, General Arnold W. Bunch avers that "our adversaries have eroded our technological advantages and have presented us with new challenges and opportunities. These adversaries are rapidly innovating, improving, and developing future technologies with new warfighting expertise. We must operate at the speed of relevance to counter these threats and develop, deliver, support, and sustain the most lethal and ready Air Force in the world."[6] A recognition of the changing nature of the threat is pervasive across the Department of Defense (DoD) and the Department of the Air Force (DAF), as is the recognition of the need for a response to counter this growing threat.

Responding to the Challenge

Operationalizing this strategic vision requires an effective information flow across the acquisition lifecycle. General Bunch's AFMC Strategic Plan recognizes this: "Our decision-makers need to be fully threat informed, and the National Defense Strategy (NDS) directs us to rap-

---

[5] Brown, 2020, p. 6.

[6] Arnold W. Bunch, Jr., *AFMC Strategic Plan*, July 2020.

idly respond with higher-fidelity threat information tailored to our customers' needs." Further, the AFMC Strategic Plan includes developing "a recurring process to communicate command-wide comprehensive threats-to-acquisition to AFMC senior leaders and program offices to ensure the command is fully threat-informed."[7]

Ensuring that acquisition is threat-informed starts before the acquisition stage, at the point when requirements are set. Requirement developers need information on the threat when they describe the initial capability needs. Requirements developers and the acquisition program managers (PMs) then need to be continuously informed of evolving adversary capabilities that relate to their specific requirements and programs so that they can respond to this evolving threat.

Being informed of the threat is not adequate to change acquisition outcomes, of course. The requirements community and PMs need to adapt—and need the resources to be able to adapt—to the changing threat over the life cycle of the acquisition, a challenge that grows more difficult the farther along in acquisition the program is. Arguably, the greatest challenge to this is that the acquisition community is evaluated on how well it meets cost, schedule, and requirements performance metrics, rather than on how well the program counters the adversary threat. To a large extent, changes to address new threats must come from the requirements community. If requirements are not adjusted, the acquisition community cannot unilaterally change them and thus must still meet the existing cost, schedule, and performance requirements. There is some flexibility within the existing requirements—key performance parameters and key system attributes—in engineering details to address some threats, but the major performance parameters are given to the acquisition community as fixed goals.

Furthermore, the acquisition community itself is not an intelligence collector or disseminator; it does not have the experience, training, tradecraft or tools—let alone the authority and responsibility—to do so. It necessarily relies on outside actors for information and intelligence. The U.S. Intelligence Community (IC) is tasked to collect, process, exploit, and disseminate the relevant intelligence data or

---

7 Bunch, *AFMC Strategic Plan*, July 2020.

finished intelligence analysis necessary for decisionmaking and incorporation into acquired systems. (The IC does support force modernization as part of its mission set, although the extended timelines to inform acquisition programs versus the more urgent needs of intelligence support to the warfighter and policymaker can make it seem that supporting acquisition takes a back seat.) And while parts of DAF have IC elements and contributions (e.g., Air Force Intelligence and particularly the National Air and Space Intelligence Center [NASIC], which plays a strong role), other intelligence relevant to Air Force requirements and acquisition is produced by organizations outside DAF.

This report discusses these challenges. To ensure that there is a focus both on the individual participants as well as the larger environment in which they operate, we refer to the "acquisition intelligence enterprise ecosystem." We focus on investments and improvements inside specific organizations, as well as on the larger structure and connective tissue that integrate their outputs toward the desired outcome of ensuring air superiority. We suggest that a system-wide view will yield a larger-scale change that is specific, measurable, attainable, realistic, and tangible—and will make a more significant difference and greater effectiveness against U.S. adversaries. The "mental model" for threat-informed acquisition includes a requirement that is threat-informed, an acquisition program that is designed so that it can be updated as the threat changes the requirement, and a flow of information to key stakeholders so the changing threat is well understood. Since every acquisition program is different, the details of the approach will differ for every program. The goal of an approach that looks at the bigger picture is to ensure that there are structures and processes in place that work together to ensure that acquisition is in fact threat-informed.

To be clear, there is no single, simple answer to the problem of incorporating intelligence into acquisition efforts. In fact, there is no answer that will fully resolve this problem. There are, however, many things that can be done to resolve various aspects of this problem that, when taken together, will improve Air Force acquisition efforts by including more and better quality (more focused) intelligence. There is also a temporal aspect to this challenge like other intelligence issues. There is no such thing as perfect intelligence; there is no crystal ball.

Additionally, the best intelligence possible provided too late in the acquisition cycle provides less than the best value, and possibly little value at all. Our goal in this report is to reflect on the challenge and offer recommendations for improvement. That said, readers may see specific examples that don't align with their own experiences. It is difficult to capture the entire range of experiences in a summary report, so we ask the reader to keep in mind the larger intent of the report, which is to provide recommendations for the Air Force to consider improving the value that intelligence can and must provide to Air Force acquisition efforts.

We note that the Air Force is not standing still. As we conducted this analysis, AFMC Intelligence Directorate (A2) and others in the Air Force continued pressing to push acquisition to become more threat-informed. New initiatives such as the Materiel Intelligence Enterprise Strategic Plan and the instantiation of directors of intelligence (DoIs) at the program executive offices (PEOs) have focused attention on incorporating threat information into acquisition.

Other Work on the Topic

This report joins a variety of other work on the topic. Perhaps the most inspiring past research has come from case-study examinations of threat-inspired acquisition, which offer fascinating examples of how specific challenges encouraged innovative designs. *Skunk Works* described how the U-2 was designed to overfly the Soviet Union and how the investments in stealth were driven by the need to have aircraft that could avoid Soviet radar.[8] *A Fiery Peace in a Cold War* describes the development of the intercontinental ballistic missile as a deterrent against the same Soviet adversary.[9] These fascinating case studies—and others—tend to focus more on the history of technology and less on the more prosaic details of requirements and acquisition manage-

[8] Benjamin Rich and Leo Janos, *Skunk Works: A Personal Memoir of My Years at Lockheed*, New York: Little Brown, 1996.

[9] Neil Sheehan, *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon*, New York: Vintage, 2009.

ment, such as DoD process improvements, which might have produced equally important benefits to the United States.

More process-oriented research on incorporating intelligence into acquisition dates from 1995 with the publication of the RAND Corporation report *Ensuring Adequate Intelligence Support for the Acquisition of New Weapon Systems*.[10] Issues identified in that report include: (1) coordination problems, (2) cost-savings measures that reduced the role of intelligence, and (3) a lack of a framework that optimized tradeoffs among acquisitions design, intelligence support, and a concept of operations.

These themes were reiterated in 1999, when Headquarters Air Force (HAF)/A2 and AFMC/CC reported a "systemic deficiency" in how intelligence, the acquisition life cycle, and related intelligence costs are integrated.[11] As a result, AFMC/A2 was directed to create a new strategy for intelligence-supported acquisitions.[12] A report produced four years later by AFMC/A2 found that 30 percent of AFMC customers did not "utilize the AFMC Intelligence Support Architecture" and that 88 percent of AFMC intelligence-sensitive programs "showed active unmet intelligence requirements."[13] Shortly thereafter, AFMC formally stood up Acquisitions Intelligence at Wright Patterson Air Force Base (WPAFB) in the mid-2000s.[14] Efforts to ensure threat-informed capabilities continued through the mid-2010s. For example, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) drove numerous efforts under the Better Buying Power 3.0 initiative to "build stronger partnerships between acquisition, requirements, and intelligence communities." These efforts included reviewing and updating policy related to critical intelligence

---

[10] Myron Hura and Gary McLeod, *Ensuring Adequate Intelligence Support for the Acquisition of New Weapon Systems*, Santa Monica, Calif.: RAND Corporation, DB-125-CMS, 1995.

[11] Tim Edem, "AFMC Intelligence Squadron: Acquisition Intelligence Cost Estimating," SCEA-ISPA Joint Annual Conference and Training Workshop, 2008.

[12] Edem, 2008.

[13] Edem, 2008.

[14] Amy Rollins, "AFMC Intelligence Squadron Redesignated as 21st Intelligence Squadron," *Wright-Patterson AFB News*, October 26, 2012.

parameters (CIPs); mandating that PMs give briefs of CIPs at annual configuration steering boards;[15] requiring overarching integrated product teams and PEOs to ensure that Defense Acquisition Board reviews evaluate threats, intelligence, and CIPs to help determine whether program requirements remain valid given the threats; ensuring that financial management policies support the funding of mission data; reviews of Department of Defense Directive (DoDD) 5250.01 on management of intelligence mission data (IMD) in DoD Acquisition; improving intelligence data transmittal through the development of validated online life-cycle threat (VOLT) reports and the creation of a threat library (TL); review workforce training on support to the acquisition community; and establishing key leader positions for intelligence support.[16] A related effort situated in USD (AT&L)'s Performance Assessment and Root Cause Analysis office worked toward "Seamless Threat Awareness in Acquisition Programs."[17]

More recently, a 2016 Government Accountability Office (GAO) report investigated the role intelligence plays in the acquisition of major weapon systems and determined that intelligence input could be better integrated. Recommendations included certifications and training for acquisition personnel, improved guidance regarding data prioritization, and better communication about intelligence products. A DoD memo responding to the GAO findings concurred with the recommendations.[18] The spirit of these recommendations falls in line with

---

[15] DoDI 5000.85, *Major Capability Acquisition*, Washington, D.C., U.S. Department of Defense, August 6, 2020, p. 33.

[16] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Implementation Directive for Better Buying Power 3.0—Achieving Dominant Capabilities Through Technical Excellence and Innovation," Washington, D.C.: U.S. Department of Defense, April 9, 2015a.

[17] Gary Bliss, "Seamless Threat Awareness in Acquisition Programs," presentation slides, U.S. Department of Defense, August 20, 2015; Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Report to Congress on Performance Assessments and Root Cause Analyses," Washington, D.C.: U.S. Department of Defense, 2015b.

[18] GAO, *Defense Intelligence: Additional Steps Could Better Integrate Intelligence Input into DOD's Acquisition of Major Weapon Systems*, Washington, D.C., GAO-17-10, November 2016.

those made in this report regarding continued improvement in communication and processes among the intelligence, requirements, and acquisition communities.

Research Questions and Methodology

About the Research

To address the policy issue of how defense leaders can most effectively leverage intelligence to address the USAF challenge of providing materiel solutions that meet changing threats, we divided the research into four tasks: (1) reviewing and analyzing relevant background material, (2) investigating the current Air Force process for intelligence support to acquisition, (3) evaluating current processes to find appropriate connections between intelligence and acquisition, and (4) documenting the research results, including making recommendations for improvement.

Methodology and Data

The team focused on qualitative and quantitative research methods, including (1) reviews of policy, guidance, and relevant literatures, including selected management literature and previous work on acquisition intelligence issues; (2) discussions (both structured and unstructured) with experts, which were conducted in person before COVID-19 pandemic limitations were put in place and via tele- and video-conferencing after their imposition; and (3) a variety of other data collection.

Guidance and Literature Review

To understand the current state of the Defense Acquisition System (DAS) life cycle, we consulted official policy guidance and senior leadership messaging on threat-informed acquisitions. This included reviewing DoD, DAF, and IC directives, instructions, and manuals to understand how the intelligence, requirements, and acquisition communities are expected to interact with and support each other. We reviewed academic and business literature to understand how information is transmitted and received in organizations, how to formalize informal communication patterns, and how threats are characterized in

nonmilitary conflict environments. These literature reviews provided a set of common practices that we could apply to our recommendations. We also reviewed other literature related to the topic, including reports written by RAND colleagues and at other federally funded research and development centers.[19]

Discussions and Interviews with Subject-Matter Experts

The team held approximately 60 separate engagements (most with multiple interviewees) with subject-matter experts (SMEs) across the intelligence, requirements, acquisition, budgeting, career field management, and other Air Force, DoD, and IC entities. Usually, multiple members of the project team participated in these engagements. Some of these were conducted in-person before the pandemic-mandated shutdown. These engagements included visits to WPAFB, where we met with AFMC/A2, the 21st Intelligence Squadron (IS), and NASIC. In the National Capital Region, we met with individuals from Headquarters Air Force Intelligence Directorate (HAF A2/6), the Air Force Weapons Integration Center (AFWIC), and the Rapid Capabilities Office (RCO). Discussions with the requirements community included requirements holders at major commands (MAJCOMS) and AFWIC personnel. After the shutdown, we held additional discussions, most of which were unclassified, with a very wide variety of stakeholders. Additional information was collected in email exchanges. We held many interviews with AFMC DoIs, a relatively new billet set up at PEOs as an effort by the Air Force Life Cycle Management Center (AFLCMC)/Intelligence Directorate (IN). DoIs are typically at the GG-15 level (although as of March 2021, three are GG-14s and one is an active duty O-5) and informed on both acquisition and intelligence issues.

We held interviews and discussions with individuals at all six of AFMC's centers, including the Air Force Research Lab (AFRL), the Air Force Test Center (AFTC), the AFLCMC, the Air Force Sustainment Center (AFSC), Installations and Mission Support (IMS), and the Air Force Nuclear Weapons Center (AFNWC). The Air Force

[19] This information was located using subject-matter expertise, keyword web searches, searches at likely sites (for example, the Defense Acquisition University website), recommendations from the sponsor, and other SMEs.

RCO and individuals with Space and Missiles Center (SMC) experience also supported this research. We talked to program offices with programs of various sizes, types, classification levels, and in various phases of the acquisition life cycle. Most of the program personnel with whom we spoke were in the fighter/bomber and Command, Control, Communications, Intelligence and Networks (C3I&N) PEOs, but we connected with tanker and space program personnel as well. At the program offices, the experts we spoke with included PMs, engineers, logisticians, and intelligence focal points.

We held several discussions over the course of the project with NASIC staff, including a day-long visit early in the project. Other Air Force meetings with intelligence personnel were held with Air Combat Command Intelligence (ACC/A2) and Air Mobility Command Intelligence (AMC/A2). We also connected with the Defense Intelligence Agency (DIA). Additionally, members of our team have a combined intelligence experience of over 70 years.

The wide range of roles held by our discussants meant that no single interview protocol was useful for all our engagements. Each began with an overview of the project and introductions. For those in acquisition and requirements roles, we asked how they accessed intelligence and threat information, either "pulling it" or having it "pushed" to them. For those in intelligence, we asked how they understood and responded to the demand signal for intelligence. The diversity of this enterprise was made clear by how different each of the interviews was. While there were common themes, we gathered new information from each successive interview.

Other Data Sources

In December 2019 a team member attended the weeklong Acquisition Intelligence Formal Training Unit (IFTU), sponsored by the 21st IS at WPAFB. Several other team members attended the half-day executive version of this course. Additionally, team members attended the ACC Technology Acquisition and Sustainment Review at Langley Air Force Base (AFB) at the end of January 2020 to receive situational awareness on how acquisition programs are reviewed at the MAJCOM level within the Air Force.

Caveats: Response to COVID-19

Research limitations include those imposed by the COVID-19 pandemic, which are worthwhile to capture as a source of lessons learned for future projects conducted with limitations on travel. The original research design included analyses of acquisition-related intelligence products and in-depth case studies of how intelligence products support the selection of acquisition programs, which would trace them from the requirements phase across the acquisition life cycle. We intended to trace specific intelligence injects back to their origin, map the process of information flows, and look for improvements. These would have been enriched by reviews of guidance and (likely classified) structured discussions with stakeholders across the intelligence support to the acquisition enterprise ecosystem.

Remote working combined with limitations on travel meant that the team focused on unclassified data collection that could be conducted using open-source materials and on unclassified telephone calls with a distributed RAND team participating from multiple locations. While we lost the richness and specificity that detailed case studies tracking the individual steps of intelligence flows could provide, there were unexpected benefits to our revised approach. A refocus on unclassified process questions opened our perspective to the higher-level challenges in improving intelligence support to acquisition, instead of a narrower approach focused strictly on improving process flows. From a team perspective, holding these discussions virtually rather than by traveling to Air Force facilities allowed us to involve the entire team in data collection, including more junior staff, who, because of cost, would not have been able to travel. This allowed more team members access to firsthand data from interviewees rather than reading secondhand notes of the interviews.

Structure of the Report

The following chapter presents an overview of the "intelligence support to acquisition enterprise ecosystem," including discussions of the intelligence and acquisition communities and of investments that can

be made in them. Chapter Three describes how written guidance and senior leadership messaging informs the enterprise, with relevant recommendations. Chapter Four analyzes the process by which intelligence informs acquisition, along with limitations and suggested remedies. Chapter Five examines workforce issues involved in ensuring Air Force acquisition is adequately informed by intelligence. Chapter Six contains findings, recommendations, and conclusions.

CHAPTER TWO

The "Enterprise Ecosystem" Approach

As discussed in Chapter One, intelligence support to acquisition takes place in a complicated defense ecosystem made up of different enterprises (intelligence, requirements, budgetary, and acquisition as well as external enterprises such as the Office of Management and Budget and Congress that require intelligence to enable the acquisition of capabilities) reporting up through different chains of command.[1] They have different incentives, resource constraints, cultures, and goals and are connected through multiple pathways of varying effectiveness using a variety of systems. These enterprises are also situated in a bigger picture with outside stakeholders providing guidance, direction, and limitations. We refer to this as an "enterprise ecosystem" to highlight the participation of separate and distinct acquisition and intelligence enterprises that demand and supply intelligence information in a much larger system with participants, processes, cultures, resource constraints and so forth, existing both inside and outside DoD.

[1] In this report, the phrase "intelligence support to acquisition" describes a flow of information necessary to ensure that capability acquisition (and life-cycle management) is effectively informed about the threat so that the materiel solutions delivered to the warfighter can counter adversary systems. Note that we are talking about informing decisions on what to acquire; those decisions include not only the acquisition community, but more important, the requirements and budgetary communities that dictate to the acquisition community what to acquire and under what budgetary resource levels. Our analysis of written documentation and the stakeholder discussions revealed, however, that focusing strictly on a unidirectional process flow of intelligence information from the IC to the acquirers misses a large part of the picture.

Understanding these complexities and looking for policy improvements across the ecosystem is the first step to developing recommendations that will instantiate the changes necessary to ensure that acquisition is truly threat-informed. Without a system-wide view, evolutionary improvements in processes could occur, but not the larger-scale change that we believe is achievable through specific, measurable, attainable, realistic, and tangible changes that will make a more significant difference. In this chapter, we describe this overarching perspective. Subsequent chapters include additional specific policy recommendations for strengthening relevant aspects of the enterprises within this ecosystem, as well as improving the communication among them. Here we set the stage and identify selected findings and recommendations relating to the big picture.

Aspects of the Ecosystem Framework

Senior Leader Strategic Guidance

Messaging from senior leadership is critical in setting the stage for transformation by communicating the strategic ends for any defense process, including intelligence support to acquisition. Staff often look to the "the commander's intent" when determining their priorities. This intent can be revealed in direct messages, speeches to the staff, public talks and engagement, written memos, published articles, and the like. These can provide specific guidance and details or more generally chart the way forward. Recipients of these messages can, in some cases, understand the point clearly; in others it must be deduced. Sometimes, guidance that is specific about one point has implications for another.

For intelligence support to acquisition, we have noted that recent messaging from both DoD (as articulated in the 2018 NDS) and from Air Force senior leaders (including an August 2020 article by the CSAF General Brown[2]) as well as prior messaging from USD(AT&L) and others specifically addresses the new threat environment facing

[2] Brown, 2020.

the United States.[3] In the July 2020 AFMC Strategic Plan, General Bunch highlighted the importance of ensuring that acquisition is threat-informed.[4] This, along with related recommendations, will be discussed in more detail in Chapter Three.

Written Policy

There is a considerable amount of official defense policy and guidance relating to intelligence support to acquisition, including DoD-level directives, instructions, and manuals from the Secretary of Defense, the Secretary's principals, and the Chairman of the Joint Chiefs of Staff, as well as directives, instructions, and manuals from DIA and from service-level issuers. This policy and guidance is created outside the Air Force's control, and while leaders can advocate for or against their content, they lack the ability to change it. We also found that policy and guidance on intelligence support to acquisition did not play an important role in how the two communities collaborate; the revision of Department of Defense Instruction (DoDI) 5000.02 and related instructions prompted a revision of myriad intelligence policies that govern support to acquisition; however, intelligence support continued apace despite the absence of policy and guidance. Several interviewees were not even aware that policy on the topic existed. This will be discussed in greater detail in Chapter Three.

Policies might offer very direct instructions and levy specific requirements; they might also offer goals and guidance that indicate there is flexibility in how they are to be achieved, although a risk-averse, compliance-driven culture (in which incentives drive people to prefer being told what to do to avoid getting into trouble later) can make this difficult. The Federal Acquisition Regulations (FAR) is the classic example of statutes, regulations, and policy that were intended

---

[3] This messaging highlights that the United States no longer has unchallenged superiority in its defense capabilities. During the Global War on Terror campaign, fought predominately in Afghanistan and Iraq, DoD faced a threat that did not possess advanced capabilities. With the United States now facing challenges from near-peer competitors, a re-posture toward more capable adversaries, including Russia and China, creates new stresses on the force, especially as new capabilities are developed and acquired.

[4] Bunch, *AFMC Strategic Plan*, July 2020.

to be tailorable for different situations but the intended flexibility has been challenging to achieve because of ambiguities in how acquisition is to be done, a lack of support in the approval chain, and concern about the risks of punishment for tailoring.[5] A detailed reference for the acquisition framework can be found in the Defense Acquisition Guidebook, which covers "Big A" acquisition with the goal of providing guidance and advice connecting requirements, budgeting, and acquisition management.[6] Note, however, that this is just guidance; the primary sources must be identified and followed to understand the complete policy picture.

While there has been some policy and guidance that has directly supported the question of "intelligence support to acquisition" (e.g., Air Force Instruction [AFI] 14-111, now rescinded), for the most part policy and guidance are broader, with selected aspects that are either directly applicable to intelligence support to acquisition or require interpretation. For example, as Chapter Three will detail, requirements and acquisition community policy and guidance address the importance of intelligence for their operations, but as a supporting (but not necessarily essential) element that is incorporated only on an "as needed basis," is tied to the DAS milestones, and often provides only strategic overviews of the DAS process. Established intelligence processes discussed in formal policy documents are just starting to recognize the need for flexibility to address smaller, ad hoc requests and needs, where information and analysis provided would have a larger impact on the development of platforms and capabilities.[7] Acquisition and requirements documents focus on cost, schedule, and performance, which leads to those intelligence documents being designed to support milestone decisions in terms of "checking the box" and thereby providing

---

[5] Megan McKernan, Jeffrey A. Drezner, and Jerry M. Sollinger, *Tailoring the Acquisition Process in the U.S. Department of Defense*, Santa Monica, Calif.: RAND Corporation, RR-966-OSD, 2015.

[6] DAU, *Defense Acquisition Guidebook*, Fort Belvoir, Va.: Defense Acquisition University, August 17, 2019.

[7] DoDI 5000.86, *Acquisition Intelligence*, Washington, D.C., U.S. Department of Defense, September 11, 2020; and DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, Washington, D.C., U.S. Department of Defense, January 23, 2020.

for minimal flexibility to allow new intelligence analysis or data to lead to changes in platform capabilities. Policies, along with recommendations to update them, are discussed in more depth in Chapter Three.

Congressional Funding Challenges

A key role is played by the legislative branch, which periodically drafts bills that create or change requirements or place or remove limitations on DoD. Congress also authorizes and programs resources for the different communities and for the acquisition programs themselves.

While the federal budget allocated for defense has been generally increasing since 9/11, DoD and the Air Force do not have total flexibility over that funding. For example, Congress allocates specific amounts to acquisition programs, and the services can reprogram certain funds without notifying Congress only if they fall below a certain monetary threshold and if their total falls within the designated limits. This limits flexibility. Acquisition programs are required by law to address intelligence in acquisition strategies. Policy also stipulates that programs should incorporate flexibilities; pay attention to evolving threat; and contain requirements for assessing sufficiency of intelligence, workforce development, requirements process, tailoring what is "in" versus "out" of a program. From the point of view of an acquisition program, however, there are challenges to react to new threats in a timely way when mitigations are expensive: it might take years to set a new requirement (or change an existing one) and receive funding from Congress to support it, and in the meantime the threat has continued to develop and advance.

Planning, programming, budgeting and execution, and evaluation (PPBE) is a deliberate process that includes requesting funding from Congress. This process is structured; once funds have been authorized and appropriated, there is little opportunity to adapt them if a different or greater threat is realized. Additionally, even with an opportunity to reallocate funds, the PPBE process is difficult and lengthy. The regimentation of the PPBE process generally reduces flexibility and limits the ability to adapt to a dynamic adversary threat. These lengthy approvals, along with limited flexibility after funds have been allocated, present serious restraints. The program element structure

(absent a reprogramming) generally does not allow funds to move from lower priorities to higher priorities outside the program element, even if the threat changes and necessitates a change in response. While the DoDI 5000 series has been revised recently, there have been little to no corresponding congressional changes made to the underlying congressional authorization and appropriation process.[8]

The Role of Multiple Enterprises in Threat-Informed Acquisition

Multiple enterprises (including requirements, budget, acquisition, and the IC) participate in different aspects of intelligence support to acquisition to ensure that delivered capabilities can meet the current or future threat. We note that while the charter of this study was to specifically focus on improving the Air Force intelligence support to acquisition, not all the relevant intelligence is produced inside the Air Force. While much of it is pulled from service-level providers (such as NASIC), intelligence is also acquired from nearly all elements of the IC. Notably, these enterprises have different reporting chains of command, and the first leader with responsibility over the different aspects might be CSAF (if within the Air Force), the Secretary of Defense (if including defense intelligence organizations such as DIA, which also reports to the IC), or even the president (if including the IC's separate nondefense entities). The issue of intelligence support to acquisition would almost certainly be lost in the noise at those levels, since it necessitates coordination between entities at a lower level to ensure the desired outcome—namely, that capabilities as delivered are designed and produced with the threat in mind. That necessity for coordination exists both within the Air Force and between the Air Force and external IC components.

In this analysis, we use a "demand/supply" framework, in which the Air Force requirements and acquisition communities (in partner-

[8] As an interviewee stated, however, "Congress has recently approved a new funding approach for software to allow for extended timeframes and a separate software funding type."

ship with the budgetary community) has the "demand" for intelligence information and the IC provides the "supply" of intelligence information. Effective integration of the demand and the supply means that the key stakeholders will know about the threat and can make an informed decision as to whether to try and deliver capabilities that will fulfill warfighter needs and allow the Air Force to counter its adversaries. Poor integration will not do so. Here, we introduce the ideas and the participants as part of the ecosystem; in later chapters we offer more detail as well as recommendations for strengthening these connections.

The Demand Side: The Warfighter Requirement

While an acquisition effort begins with a concept development phase, formal acquisition programs begin at the requirements stage, which is generally conducted as a function tied to warfighting. Within the Air Force, groups at the warfighting MAJCOMs identify capabilities they need, which are then vetted, prioritized, and provided as requirements to the acquisition community. The operational commands are the "resource providers" that vet and advocate for capabilities. These capabilities might come from experience in the field or concerns about adversary capabilities driven by different forms of intelligence. The intelligence functions at the commands (A2) are critical to providing this intelligence to the warfighters and might need to reach out to the broader IC to do so.

Headquarters organizations such as AFWIC within DAF Strategic Plans and Requirements (AF/A5/8) are involved in requirements setting, which can involve wargaming and modeling and simulation (M&S) to test options against the threat. CSAF is the key requirements adjudicator for DAF, and the Joint Capabilities Integration and Development System (JCIDS) is the joint requirements piece of the three main processes supporting acquisition (the other two being acquisition management and funding). Materiel solutions are not necessarily the resulting capability to deal with the threat—it is one of numerous options as outlined in doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) analysis.

In our data collection, we held discussions with the requirements community, including requirements holders at MAJCOMS and AFWIC personnel. While our research focuses more deeply on the acquisition management–intelligence nexus, we recognize that acquisition, intelligence, and requirements work together as a "three-legged stool" in providing capability to the warfighter and that only the requirements community has the responsibility and authority to set capability requirements.[9] During our discussions, AFWIC personnel described being engaged with threat issues, but highlighted that information-sharing from the IC was not always smooth, and that without updated information, there was a risk of preparing for "fighting the last war." Conversely, an ACC requirements holder for a fighter program reported talking to their intelligence officer at least weekly as well as engaging with service intelligence centers (NASIC and Missile and Space Intelligence Center) and with national-level IC organizations. Such requirement holders also push issues to the program office. RAND Project AIR FORCE (PAF) researchers supporting U.S. Air Force wargames found that these events do have a threat focus.

PMs with whom we spoke reminded us that stable requirements made acquisition management better and easier, and that if the threat suggested significant changes to the capability, these usually connected to the requirements and thus needed approval from the requirements holder. Changing a program to respond to a threat, however, might not be the requirements setters' top priority for their resources. Thus, even if an acquisition program as designed would face challenges in responding to an evolving threat, the decision might be made that the risk must be accepted, and that acquisition should proceed as initially planned. That could be a cause of frustration along the acquisition-intelligence nexus, if the IC delivers information upon which action is not taken, but it is not the IC's responsibility to ensure that threats are mitigated. The recommendation here is for the acquisition community to continue to communicate intelligence priorities, to encourage the flow of information, and for the intelligence community to respond

[9] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2015b, p. 10.

where possible[10] despite any lack of action (which may very well be caused by resource constraints). The continued flow of information, however, is important, as priorities might change, and resources might become available in the future.

Planning, Programming, and Budgeting

As described above, resources need to be allocated to requirements and any related capability pursuit in order to start or make significant changes to acquisition programs. Getting a requirement's associated funding through the PPBE process and the congressional authorization and budget allocation process can take up to two years, depending on the priority, level of funding needed, and relevance to existing budgetary programming. It is also a competitive process—there are always more requirements than there are available resources. Even if the decision is made to increase investments in a program to meet a threat, the cycle time of the PPBE process and even a shorter-term reprogramming activity create delays because the resources are not instantly available. Additionally, the threat can further change during these delays.

The Demand Side: Acquisition Management

Once the requirement is set and funding is appropriated, programs enter the DAS, which is broad and diverse. This overview is not intended to provide a full description of the acquisition process or enterprise—which is not the purpose of the report, and would repeat information covered elsewhere. Rather, this is a broad discussion intended to highlight several of the complexities in acquisition in order to make the point that ensuring that acquisition is threat-informed requires more than a single product or discrete threads of information flow. The complexities of the acquisition system—the number and diversity of participating organizations and programs—contribute to the difficulties of identifying generalizable recommendations and of assessing the demand for

[10] There is a need to be cognizant of limited intelligence bandwidth. Acquisition programs that do not "bake-in" flexibility to respond to threat changes, and thus where there is the implicit acceptance of risk regarding staying ahead of the adversary, should be lower on the priority list for intelligence application than programs that will be able to respond to actionable information.

intelligence. There is no "one size fits all" approach that would result in effective intelligence support to programs. The complexities of the system, however, do not mean that the challenge of improving the connection between acquisition and intelligence is intractable.

AFMC—composed of a headquarters and six main centers operating at multiple locations and employing tens of thousands of personnel[11]—is the main Air Force organization responsible for managing acquisition.[12] There are also Air Force organizations designed to address more urgent needs, such as RCO, which has a separate reporting structure. AFLCMC manages most of the Air Force's acquisition programs, which are housed in PEOs, including fighter-bomber, C3I&N, tankers, agile combat support, and so forth. These acquisition organizations take direction and guidance from the Office of the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ) structure, as well as from authorities outside the Air Force such as USD (Acquisition and Sustainment [A&S]).

The Air Force manages programs through the many stages in the capability life cycle across the formal milestones—from basic research through various levels of invention, experimentation, prototyping, testing, fielding, sustainment, and disposal. Our interviewees were unanimous in the perspective that intelligence is most useful when it comes early—when requirements are being set and in a program's early design and development period, when there is still flexibility in design and before too many decisions have been made and developments undertaken.

Acquisition programs take place along different pathways.[13] Current policy has six formal acquisition pathways, from a major capability acquisition that might take from a year to a decade or more and repre-

---

[11] These are the Air Force Research Laboratory (AFRL), Air Force Test Center (AFTC), Air Force Life Cycle Management Center (AFLCMC), Air Force Sustainment Center (AFSC), Air Force Installations and Mission Support (IMS), and Air Force Nuclear Weapons Center (NWC).

[12] AFMC, "Air Force Material Command," factsheet webpage, June 2020.

[13] DoDI 5000.02, 2020; see also DAU, "Adaptive Acquisition Framework Pathways," webpage, undated(a).

sent an investment of tens of billions of dollars to a software acquisition that might cost less than a million dollars and take months (and that, in spite of its small size, might represent a critical capability) or cost billions and take many years.

There are different contracting approaches. Some have more flexibility—such as cost-reimbursement contracts, which reimburse industry for "allowable incurred costs, to the extent prescribed in the contract," often with a fixed fee.[14] In others, the contractor provides a deliverable "for a firm price or, in appropriate cases, an adjustable price."[15] Each approach has strengths and limitations. More flexible contracts pose the risk of greater price growth to the government due to fewer price controls and incentives, but at the same time, these may be easier to adjust to respond to changing requirements, including those that arise as a result of new intelligence on the threat. More restrictive contracts, such as those that are fixed price, provide a strong incentive to control costs through price controls, but they can be more work when making changes to deal with new requirements, including those that may arise as a result of changing intelligence.

The number and seniority of personnel inside program offices—civilians, officers, enlisted, and contractor support staff—vary. So do their roles, which can include PMs, contracting officers, cost analysts, and engineers. Some programs have intelligence personnel embedded in their programs or have intelligence focal points; others are less connected to the IC. We address workforce issues in more depth in Chapter Five.

Air Force Support for Diversity-of-Effort Challenges

The diversity of the acquisition enterprise was reflected in the variety of acquisition efforts with which we connected. Some programs were very highly "intelligence sensitive" while others not involved with intelligence-sensitive programs were unfamiliar with the term. They were at differ-

---

[14] FAR, Part 6 - Competition Requirements, Subpart 6.3 - Other Than Full and Open Competition, 6.301 - Policy, March 10, 2021.

[15] FAR, Part 16 - Types of Contracts, Subpart 16.2 - Fixed-Price Contracts, 16.201 - General, March 10, 2021.

ent phases in their life cycle and thus able to shape acquisition based on new or emerging threats in different ways. Some reported being limited by the design and progress to date, while others (especially cyber-related efforts in C3I&N) were more able to adapt. As we worked to develop recommendations, we quickly realized that the different structures, challenges, and constraints meant that recommendations had to be as broad as possible in order to cover as much of the enterprise as they could and be broadly applicable. This finding links to a recommendation that those charged with ensuring effective threat-informed acquisition (perhaps HAF A2/6 and AFMC/A2) recognize and communicate to the broader Air Force that broader support and resources are required to keep pace with evolving threats. The corollary to this is that the rest of the Air Force needs to recognize where it can play critical roles and provide support to these future warfighting systems. Alternatively, some options for improvement have to be tailored to individual situations; in these cases, broad recommendations are not possible or advisable and can lead to other problems.

Acquisition Intelligence Housed Within the Air Force Materiel Command

Most U.S. Air Force acquisition programs are housed within the Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ) PEOs and under AFMC for operational testing and evaluation (OT&E) functions. As is the case with other MAJCOMs, AFMC's command structure includes an intelligence function (AFMC/A2), and AFMC has a dedicated intelligence squadron in AFLCMC (the 21st IS) devoted to ensuring intelligence supportability for Air Force systems.[16] AFMC also includes approximately a dozen organizations with intelligence personnel who support the

[16] Chairman of the Joint Chiefs of Staff Instruction J8, *Manual for the Operation of the Joint Capabilities Integration and Development System*, August 31, 2018. B-G-G-1 defines intelligence supportability as ensuring "that capability solutions are developed in the context of applicable adversary threat capabilities, that intelligence requirements have been identified and documented at the earliest possible point, and that all likely intelligence support requirements and shortfalls (if applicable) have been assessed for availability, suitability, and sufficiency."

acquisition mission. AFMC/A2 has recognized the importance of, and challenges inherent in, intelligence support to acquisition and has undertaken numerous initiatives to improve what it refers to as the "Materiel Intelligence Enterprise" (MIE). AFMC/A2 support some 740 programs (including some AFRL projects), with the minimum being annual contact to PMs.[17]

Here we discuss their recent efforts to invest in improving acquisition intelligence.

Materiel Intelligence Enterprise Strategic Plan

AFMC/A2's efforts over the last several years have included creating a new MIE strategic plan.[18] This plan includes the following:

- MIE definition: "the sum of all forces and infrastructure providing federated intelligence (support and analysis) in AFMC, including in capability development and program offices"
- MIE vision: "a ready, relevant, Materiel Intelligence Enterprise delivering agile and risk-managed ISR [intelligence, surveillance, and reconnaissance] support to the acquisition lifecycle and installation management"
- MIE problem statement: "Policy, resource, communication and cultural constraints, as well as Acquisition Community lack of awareness of Materiel Intelligence Enterprise Value far left of need reduces our ability to fully support and inform acquisition efforts at the speed of relevance."

Not surprisingly, the MIE strategic approach emphasizes the many aspects of intelligence support to acquisition that can be affected by policy within AFMC, which oversees the majority of Air Force acquisition (at least the larger programs as measured by dollar amount). In our stakeholder discussions we found that the MIE strategic plan was somewhat known in the acquisition community, so AFMC/A2's efforts to communicate the strategic nature of the issue is percolating. A rec-

[17] AFMC/A2 provided a list of relevant programs to the project team.

[18] AFMC, "AFMC's Materiel Intelligence Enterprise Strategic Approach," pamphlet, undated.

ommendation based on this is for AFMC/A2 to continue to stress the strategic nature of the MIE, and for AFMC senior leadership to provide or advocate for resources for aspects of the plan, as priorities allow.

Directors of Intelligence

One MIE innovation has been AFLCMC/IN's effort to develop and instantiate a DoI concept whereby a person or a small team of people who understand acquisition intelligence is co-located at the PEO with the DoI director and is responsible for supporting intelligence information flows to acquisition programs and serving as a resource for reach back to the IC. The goal of this structure is to have a single touchpoint for intelligence for acquisition programs so that they can better access intelligence and get their questions answered. DoIs can also provide a crossflow of information among programs and push relevant information to programs. Discussions with selected DoIs revealed that they most often were senior civil servants with extensive experience and personal contacts across the ecosystem. They were able to point to instances of sharing information and answering questions. Many of the acquisition programs also knew who their DoIs were and indicated that they were a helpful addition. The caveat to this is that DoIs are a relatively new structure. Many DoIs with whom we spoke had started in the position in the spring of 2020, during the pandemic, and so were less able to serve as a connection for significant classified issues due to remote-work constraints. Further, as a relatively new structure, they had few successes along the lines of "We informed an acquisition program about a threat, the program was updated, and the resultant capability was successful." That said, overall, DoIs received support from acquisition and seem to be a promising practice. One interviewee working in a DoI office pointed out that being located in the PEO allowed them to influence priorities and funding so that if "you run out of resources literally at the margins, . . . you go to the next least important programs"[19] Our recommendation is that investments continue to be made in the DoI concept (as resources allow) and that it become a standard part of the PEO structure.

[19] SME interview, May 27, 2020.

The Supply Side: The Intelligence Community

The IC produces and validates intelligence data and products. It represents the "supply" side. Much like the acquisition enterprise, the IC is a complex environment, with multiple organizations producing different kinds of intelligence and operating at different levels of classification. Acquisition is just one of the general missions that the IC supports—and the numbers and broad needs of consumers of intelligence result in competition for intelligence. DIA manages the Defense Intelligence Analysis Program (DIAP), which integrates the different types of intelligence across the many producers. There are various intelligence producers (NASIC, DIA, National Geospatial-Intelligence Agency [NGA], and other technology and long-range analysis (TLA) offices) producing a myriad products. NASIC is the Air Force's organic source of military intelligence for foreign air and space threat analysis.[20] Air Force acquisition personnel most frequently referred to NASIC when they discussed the IC—one expert suggested that 80 percent of the intelligence used by the U.S. Air Force came from NASIC. Conversations with NASIC personnel revealed that their most important mission was supporting the national intelligence mission, more so than acquisition, and indicated that they did not have the resources to respond to every request in a timely way. Understanding priorities is one of the reasons why understanding the broader ecosystem is critical. A perceived simple "solution" of adding additional staff to NASIC to improve intelligence support to acquisition might be expeditious; however, it might not produce the desired results, as the priority might be higher for new members of the workforce to support current operations instead of acquisition. This issue is described in greater detail in Chapter Four.

---

[20] DoDD 5000.01, *The Defense Acquisition System*, Washington, D.C.: U.S. Department of Defense, September 9, 2020, clarifies the broader authority and responsibility from U.S. Code, Title 10, Section 137, Under Secretary of Defense for Intelligence and Security, to produce intelligence in support of acquisition. It indicates that, under the authority, direction, and control of USD(I&S), the directors of DIA, NGA, NRO, and DCSA and the NSA chief for Central Security Service provide intelligence support to acquisition related to their specific areas of responsibility.

Integrating Supply and Demand: How Acquisition and Intelligence Connect

The acquisition intelligence ecosystem has both formal and informal layers that interact to influence policy and operational decisions. The formal layer includes the VOLT assessment,[21] an intelligence document that is required by policy and aims to support decisionmaking at key points in the acquisition process.[22] This layer also includes intelligence production requirements that are officially tasked to designated producers through tasking systems such as the Community On-Line Intelligence System for End Users (COLISEUM). Another formal layer is TWGs or TSGs, which are empaneled at PEO or program levels and are critical forums where program and intelligence support officers meet to discuss and formalize intelligence support requirements.

The informal layer—which is larger and has important, albeit undefinable, influence—is the web of relationships among members of the ecosystem who consistently depend on unstructured networks for information that they trust and that can be acquired more quickly than through the formal task-response system. Connections in the informal layer range from simple clarifications to deeper conversations can help appropriately shape formal requests.

Our descriptions of the acquisition community's demand for intelligence and of the IC's supply of intelligence should demonstrate the complexity of the effort to make threat-informed acquisitions. Because it is so difficult to measure and thus understand the level of demand, meeting it is a challenge—one that cannot be resolved by adjusting individual elements. As a representative from the IC put it, "We're still challenged to become a part of the fabric of Acquisitions. . . . If we're perceived to be providing interesting intel but not perceived to be adding value for decision making, then we will never become . . . a routine practice in Acquisitions."[23] Similar sentiments were felt on the acquisitions side: "Our failure to prioritize has impacted the ability of

---

[21] We provide a broader discussion of the VOLT requirement later in the report.

[22] DoDI 5000.86, 2020 and DoDI 5000.02, 2020 now provide for VOLT to be optional.

[23] SME interview, April 24, 2020.

the Intelligence Community to serve us because they can't prioritize intelligence in a way that serves us best. When everything is important, then nothing is important. Acquisition's failure to construct a clear demand signal to the IC has hurt Intel's ability."[24] The lack of a strong integrating function (i.e., a single senior decisionmaker having authority over both enterprises and possessing sufficient capability to work the effort) means that creative solutions beyond those that merely rely on central authorities' guidance or directions should be sought. Chapter Four describes this challenge and offers specific recommendations.

Other Aspects of the Ecosystem

Understanding the challenges inherent in connecting the acquisition and intelligence enterprises within this broader structure is not just about the organizations and the processes for ensuring information flows. There are other aspects that warrant discussion, as they shape the nexus between acquisition and intelligence.

Cultural Differences

In the acquisition community, participants manage with the objective of increasing certainty even if the environment is uncertain. The requirements community and acquisition PMs seek to reduce uncertainty early on by getting as much firm intelligence as possible on the long-term threats so as to structure the program and set the requirements and designs correctly in the first place. Changes later are costly and may not even be possible for technical or budgetary reasons, so the objective is to set up the program correctly from the start.

Within the IC, in contrast, there is an ongoing tolerance of uncertainty, which is expected and understood. Driving toward certainty misses the point that the adversaries are also evolving. We were told during our interviews that acquisition professionals can be frustrated by a lack of definitiveness on the part of their IC counterparts, while they in turn can be frustrated by the acquisition community's request

[24] SME interview, April 20, 2020.

for unknowable or specifically defined information. One interviewee summed up the challenge: "We get a couple million dollars in funding every year from programs to do very specific support, which is unfortunate because I think it's the type of support the intel community is capable of providing and is funded for but the intel community is too slow and doesn't provide analysis at the appropriate level of fidelity that's actionable by a program office."[25]

Incentives

For programs with little flexibility to evolve under agile development practices, the acquisition community is judged by the three metrics of cost, schedule, and performance against the original and the latest requirements and baselines. These are important management considerations, but this approach neglects how well the program is postured to meet the evolving threat. New intelligence on threats is "bad news," not just because of the increasing capabilities of the adversary, but also because of the potential impact on the program's management metrics. As one former PM put it, "You need both continuous and early [intelligence]. . . . PMs are judged against [the Acquisition Program Baseline] APB to meet cost, schedule and performance. Intel can be seen as a disruptive force for meeting the APB, so PMs would resist changes driven by Intel changes."[26] There might not be additional available resources, or the program might not be the priority of the requirements setter, so the program might be told to risk not being able to counter the new threat. In other words, it is largely not the job of the acquisition community to address all threats because they do not control requirements and budgetary resources. They should raise these issues, address what they can within their limited flexibilities, and advise the requirements and budgetary communities of the implications and options for addressing threats, but in the end, they are held to deliver only on the assigned requirements given allocated budgets.

Assessing PMs' performance against an evolving threat is problematic, because so much is out of their control. One possible solution

[25] SME interview, May 6, 2020.

[26] SME interview, April 21, 2020.

here could be to set aside some sort of other management reserve that could be applied depending on evolving threats—although preserving management reserve against unknown threats when there are competing priorities could be a naive hope given the difficulty of arguing for budgets with Congress for an unknown, as well as the vulnerability of such a management reserve to the comptroller's ever-present search to find and reprogram resources to address threats elsewhere in DoD. Another approach could be to focus on the process by which information is handled. For example, was it shared with the requirements setter or holder to ask for reprioritization? Were resources requested? A focus on process (e.g., cost, schedule, performance) rather than outcomes is certainly less satisfying, but PMs need incentives to continue to elevate considerations of the threat, even though we cannot, in the end, hold acquisition professionals accountable for issues outside their control. An additional challenge is that the length of time it takes to develop and manufacture complex systems combined with personnel turnover mean that assigning responsibility to individuals for the distant outputs of their programs (when the PMs, at least, will probably be long gone) can be difficult if not impossible. That said, acquisition PMs have a general responsibility for system performance given warfighter needs, and PMs take this seriously and at least try to address these concerns through venues such as the configuration steering boards and discussions with requirements holders and budgetary planners. Addressing the enterprise ecosystem as a whole, continuing to work to ensure that the acquisition programs are threat-informed throughout their life cycle, might be the necessary response.

Incentives on the IC side can also lead to missed opportunities. For example, we heard that IC analysts may be evaluated on the percentage of production requests that they address or "close." If pervasive, this simple metric does not link to how effectively or thoroughly acquisition customers are supported, and it could lead to the reshaping of requests so that they are addressable with existing information, thus making true demand for intelligence impossible to ascertain. This is discussed in greater detail in Chapter Four.

Difficulties in Assessing "How Much Is Enough?"

Another challenge of the ecosystem—and of improving it—is the difficulty of knowing the true demand signal. Determining "how much is enough" turns out to be quite a difficult task. There is a top-down goal set by leadership of having threat-informed acquisitions and a bottom-up signal created by the requirements community and PMs as expressed in the required acquisition-related intelligence products.[27] These will be discussed in more detail in Chapter Four, including some of their inherent challenges in developing metrics for whether the IC meets demand given the many uncertainties.

Additional Findings and Recommendations

Experts and stakeholders with whom we held discussions consistently informed us about issues that are beyond their control but that shape the ability of intelligence to be informed by acquisition needs or of acquisition to incorporate intelligence information. As we continued the research, the picture became clearer: We came to understand that threat-informed acquisition is shaped, supported, and limited by the complexities found in the organizations in which our interviewees work and in entirely separate enterprises. The main implication of this is that the challenge of ensuring threat-informed acquisition is not something that can be controlled or addressed entirely by our sponsor, AFMC/A2, or the Air Force headquarters intelligence function (HAF A2/6), or even within the Air Force.

A significant recommendation derived from this finding is that if threat-informed acquisition is a goal of the Air Force—and guidance from senior leaders suggests that it is—then this will require ongoing senior leader support and appropriate resourcing.[28] At present, HAF

[27] DoDI 5000.86, 2020 directs sufficiency assessment and the Chairman of the Joint Chiefs of Staff Instruction 3317.01, *Intelligence Oversight Responsibilities, Procedures, and Oversight Functions*, January 6, 2020: process articulates how much is enough to meet critical mission needs for select types of intel data: EW, characteristics and performance, signatures, M&S.

[28] We note that in a resource-constrained environment, additional resources might need to be moved from other areas and that that these trades would need to be made by USAF leadership.

A2/6 and AFMC/A2 are playing a lead role in developing solutions and should receive this support as the overall resources and other priority allow. Additionally, USD(A&S) and USD(Intelligence and Security [I&S]) are continuing to issue policy to pursue threat-informed acquisition, which should prove beneficial.

Finally, we note that the program portfolio and acquisition system components are fluid over time. New acquisition programs are initiated, and others finished. Perhaps more important, staff move around. PMs often get their start in smaller, less sensitive programs and gain increasing responsibility over time until they are managing large, risky programs. Ensuring that even the less sensitive programs are and know how to be "threat-informed"—aware of potential adversary systems even if from the big picture rather than directly linked to their program; and considering how well their programs address potential threats along with meeting cost, schedule, and performance metrics—will ensure that PMs and their staff will get the grounding they need in a threat-informed culture to ensure a consistent thread of this perspective throughout their careers.

CHAPTER THREE

Department of Defense Policy Guidance and Leadership Messages

This chapter examines official policy guidance and senior leadership messaging on threat-informed acquisitions. It summarizes and analyzes relevant guidance through the optics of three communities: intelligence, requirements, and acquisition, and their perspectives on threat-informed acquisitions. Throughout the chapter, the project team highlights the relevant touchpoints between intelligence, requirements, and acquisition. This summary and analysis include observations regarding relationships among the three communities, activities pertaining to the use or provision of intelligence data and threat information, and any inconsistencies among current policies that could prevent holistic integration of all three communities into a program's life cycle or its adaptation to future threats.

Our project team reviewed DoD-level directives, instructions, and manuals from the USD(A&S) along with Chairman of the Joint Chiefs of Staff directives to understand how the subordinate-level intelligence, requirements, and acquisition documents related to larger policies and objectives. On the intelligence side, we read directives, instructions, and manuals from USD(I&S), DIA, and DAF, illuminating how the IC provides necessary analysis and information to the acquisition community. From discussions with people in the acquisition and requirements communities, we learned how and when those communities expect intelligence inputs to support DAF acquisitions through their instructions, manuals, and handbooks. Public statements of senior DoD and DAF officials provided additional insight

into current thinking about the relationship between Air Force acquisition and the intelligence that supports it.

In describing the geopolitical world that the United States expects to be confronting, the 2018 NDS addresses the need for an intelligence-driven acquisition process.[1] It explicitly states:

> The security environment is also affected by *rapid technological advancements and the changing character of war*. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed.[2]

Further, it highlights that long-term strategic competition necessitates "the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military."[3] In identifying all of the members of the strategic ecosystem, NDS reminds us about their interdependence and the criticality of each part to achieving U.S. strategic objectives. It further emphasizes that the U.S. military must "anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us" by defining and assessing our technologies and anticipated future conflicts while fostering experimentation and environments that encourage risk-taking.[4] For acquisition and requirements to achieve those goals, intelligence is critical.

This chapter traces how intelligence policy considers acquisitions and vice versa. We start with intelligence from a threat-informed perspective, as it should provide the foundation for requirements and acquisitions. The policy and guidance generally recognize each community's ecosystem. Both requirements and acquisition communities address the importance of intelligence as a supporting element for their operations—it is not a co-equal element of the life cycle. Requirements and acquisitions documents, along with the budgeting process, are fre-

---

1 DoD, 2018a.

2 DoD, 2018a, p. 3 (emphasis in the original).

3 DoD, 2018a, p. 4.

4 DoD, 2018a, p. 7.

quently referred to as the core of the DAS life cycle. Intelligence has processes to support the DAS, with the formal structures discussed in the guidance being tied to major DAS milestones. There is much less detail in the guidance recognizing the need for flexibility to address smaller, ad hoc requests and needs. The connective tissue between the communities exists but needs reinforcement as threat-informed acquisitions become the norm.

Policy Review Through the Intelligence Lens

Three key elements emerge from a review of intelligence documents discussing intelligence support to acquisitions. First, DAF manuals and instructions provide direction to the acquisition and intelligence communities on how the two should interact, but the onus remains primarily on DAF intelligence analysts, who provide support to acquisitions to push products or engage with acquisition or requirements communities. Second, intelligence policy documents (from both DIA and DAF) focus on internal intelligence processes and product development rather than how specifically defense intelligence organizations and their products fit into the DAS.[5] Third, intelligence and counterintelligence (CI) analysis is required to support the DAS, but it is handled in different channels. At the DAF level, CI support is the responsibility of the Air Force Office of Special Investigations (AFOSI), not intelligence, whereas at the DoD level, DIA has both intelligence and CI responsibilities. This split could lead to stove-piping and collaboration gaps, preventing holistic threat assessments to support the DAS.

Department of the Air Force Instructions and Manuals

DAF develops and maintains guidance on the interaction between intelligence analysts and the acquisition community. In recent years, however, the focus on streamlining guidance documents has affected the specificity of interactions between the acquisition and intelligence communities. For example, the guidance document with the most spe-

[5] As a result, most of the discussion regarding how intelligence production fits into the DAS will be covered in that section, mirroring official DoD and DAF guidance documents.

cific and detailed information for this relationship, AFI 14-111, *Intelligence Support to the Acquisition Life-Cycle*, was rescinded in 2019. Acquisition intelligence analysts continue to refer to AFI 14-111 due to the detail provided about their responsibilities. Air Force Manual (AFMAN) 14-401, *Intelligence Analysis and Targeting Tradecraft/Data Standards*, is the instruction's replacement; however, it lacks most of these details.[6]

AFI 14-111 discussed the role of intelligence support from SAF/AQ; HAF A2/6 and HAF Operations, Plans, and Requirements Directorate (HAF/A3/5); MAJCOMs; PEOs and PMs; and the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) (through NASIC), AFMC/Air Force Space Command (AFSPC), the Air Force Operational Test and Evaluation Center (AFOTEC), and AFOSI as it specifically relates to the acquisition community.[7] AFMAN 14-401 supersedes 14-111 and other AFIs on targeting, tactics analysis, and reporting, intelligence analysis, and intelligence analysis and production, leading to a more general document on DAF intelligence support. AFMAN 14-401 provides only general statements directing various DAF intelligence elements (HAF A2/6, NASIC, MAJCOM A2s, and the commanders of AFMC and AFSPC) to support the requirements and acquisition communities, often highlighting those communities' policy documents versus intelligence-based ones. Thus, DAF intelligence documentation continues to focus on how internal procedures operate once requests for information arrive to them, as opposed to the connective tissue between intelligence and the DAS elements.

In fact, AFMAN 14-401 provides the most detail to the commanders of AFMC and AFSPC, who are to "guide the integration, synchronization, and advocacy of intelligence support to research and development, acquisition, test, sustainment and installation management."[8]

---

[6] Acquisition Intelligence Formal Training Unit (IFTU) course, Wright-Patterson Air Force Base, December 2019, student notes.

[7] AFI 14-111, *Intelligence Support to the Acquisition Life Cycle*, U.S. Department of the Air Force, Incorporating Change 1, June 16, 2014, pp. 3–9.

[8] AFMAN 14-401, *Intelligence Analysis and Targeting Tradecraft/Data Standard*, U.S. Department of the Air Force, August 8, 2019, p. 9.

The manual, however, lacks details beyond that; instead it directs further attention to DoDI 5000.02, *Operation of the Defense Acquisition System*, DoDI 5000.75, *Business Systems Requirements and Acquisition*, AFI 63-101/20-101 *Integrated Life-Cycle Management*, and the JCIDS Manual. Of note, these are DAS documents, not intelligence documents. By making intelligence a supporting entity to be utilized to the greatest extent, a commander or PM must be engaged and recognize the criticality of intelligence to requirements and acquisition. Intelligence alone cannot drive support to the DAS processes; this will be discussed further in the requirements policy and acquisitions policy sections.

To be effective, intelligence support to acquisitions must be relevant, iterative, tailored, and collaborative.[9] While each of these tenets is critical, the iterative and collaborative nature of the relationship cannot be overemphasized. The expansive breadth and depth of the life cycle of an acquisition program—which includes developing a requirement, overseeing system development and production, testing and fielding, and sustaining and maintaining processes—underscores these collaborative interactions. Intelligence documents emphasize *what* intelligence provides and *how* it conducts analysis, while acquisition documents highlight *when* intelligence provides that analysis (i.e., as specified in the DAS policies and guidance, during the phases between the milestones and to inform content in various documents reviewed at milestones).[10]

AFI 14-111 provides the following example. PMs and their intelligence support should be working together throughout the life cycle, first to determine if a program is intelligence-sensitive, then whether it produces, consumes, processes, or handles intelligence information or whether it requires intelligence personnel during program development or mission execution.[11] When a program is deemed intelligence-

---

[9] AFI 14-111, 2014, pp. 2–3.

[10] While the DAS-related guidebooks discuss intelligence support to acquisitions, they are written to provide guidance to PMs and PEOs and not intelligence professionals. Discussion of ad hoc RFIs to the IC reflect the need to seek answers related to progress of a program between milestones. See DAU, 2019a, chap. 7.

[11] Acquisition IFTU course, Wright-Patterson Air Force Base, December 2019, student notes, 2019; AFI 14-111, 2014, p. 9.

sensitive, an intelligence supportability assessment is conducted. This is the process by which DAF intelligence, acquisition, and operations analysts identify, document, and plan for requirements, needs, and supporting intelligence infrastructure that are necessary to successfully acquire and employ Air Force capabilities, thereby ensuring intelligence supportability. It is an iterative, collaborative process that provides tailored support to intelligence sensitive efforts.[12]

The IC often remains in a position of "pushing" intelligence to Air Force PEOs and PMs, who are the key "pullers" of intelligence into the DAS process. The standard process documents published by AFLCMC—titled *Intelligence Sensitivity Determination* and *Intelligence Supportability Analysis*—delineate acquisition, requirements, and intelligence roles in requesting intelligence assessments when new programs are established.[13] Out of nine possible "entry" points for intelligence to provide input, only one is a clear "pull" with one other possible "pull" by the PM; the remaining are either intelligence "pushes" or some combination of "push/pull."[14] This breakout indicates that the IC must remain proactive to ensure that it is included from the beginning of a program, which can have implications for its ability to provide continual support to programs. If threat intelligence is not recognized at the beginning by the PM or PEO, it is harder to incorporate the information later in the DAS process; this, in turn, can discourage the PM from regularly communicating with the IC and incorporating intelligence data and analysis.

---

[12] AFI 14-111, 2014, p. 9.

[13] AFLCMC, *Standard Process for Intelligence Sensitivity Determination*, Version 3.2, April 19, 2018; AFLCMC, *Standard Process for Intelligence Supportability Analysis*, Version 2.0, September 19, 2019.

[14] The PEO or PM "pulls" include notification or request to supporting intelligence division, which is a significant programmatic change that would require an intelligence sensitivity determination reassessment. The "push/pulls" include approval of new work through the AFLCMC corporate process; discovery of new work through formal/informal coordination of/with JCIDS documents, DAS documents, AFWIC, or MAJCOMs. The intelligence "pushes" include discovery or notification of new work on an acquisition master listing, which is a significant change to a threat environment which would require an intelligence sensitivity determination reassessment. AFLCMC, 2019, pp. 4–5.

Intelligence Guidance

Looking at intelligence support to acquisition through the strategic level lens, IC policy and guidance prioritize the discussion of processes: working groups, producing threat assessments, and maintaining databases for finalized and approved production. Often, these processes are internal to the Defense Intelligence Enterprise (DIE), but the working groups, for example, also include representatives from the acquisition community.[15] Intelligence documents refer to acquisition or requirements community guidance for specific milestone events requiring intelligence and threat assessments. DoDI 5000.02 *Operation of the Defense Acquisition System*, DoDI 5000.86 *Acquisition Intelligence*, the JCIDS Manual, *DoDD 5105.21 Defense Intelligence Agency,* and DIA's Intelligence Threat Support to Acquisition Guide 5000.2-1[16] all delineate the role of DIA and intelligence production centers (such as NASIC) in providing intelligence information and assessments,[17] support to testing and evaluation (T&E) and M&S efforts, and counterintelligence (CI) assessments for Major Defense Acquisition Programs (MDAPs) (specifically acquisition category (ACAT) 1D).[18]

There are two primary types of intelligence that the IC provides to the DAS: intelligence mission data (IMD) and information and threat assessments. IMD are specific data required both by programs to support T&E, M&S, and so on, and by operating platforms to accomplish their mission. Analysis of the strategy and intentions of a foreign adversary is included in threat assessments. IMD remain critical throughout the entire life cycle of a platform, including development, testing, and sustainment, but especially in operation. IMD is required for the

---

[15] DIAI 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, February 1, 2013.

[16] DIAI 5000.002 was rescinded in 2019. The replacement takes the form of a Guide instead of a regulation or instruction. The draft document is currently being used unofficially to guide support to acquisition efforts.

[17] Specific intelligence documents and data produced in support of the DAS will be discussed in depth in Chapter Four.

[18] DoDI 5000.02, 2020; DoDD 5105.21, *Defense Intelligence Agency*, Washington, D.C.: U.S. Department of Defense, March 18, 2008; DIAI 5000.002, 2013.

system operator to determine the threat facing it and then be able to prepare an effective response to achieve the military mission.[19] DIA runs the Intelligence Mission Data Center (IMDC) as the focal point to develop, produce, and share IMD across the services. Moreover, IMDC specifically provides information on the data availability, costs, architecture, compatibility, and standards for acquisitions programs.[20]

Primary threat assessments are provided in VOLT reports, which are written by the service intelligence centers and validated by DIA.[21] DIA also maintains the online repository for VOLT reports, which is called the Defense Intelligence Threat Library. This database is the primary threat-assessment tool used to support milestone decisions by informing the capability-development and mission-needs phases against foreign threats.[22] VOLTs are to be leveraged throughout the initial determination phases for developing or updating new capabilities and deciding whether a materiel solution is necessary (initial capability document [ICD]), and at each milestone requirement (capability development documents [CDD]). The technology targeting risk assessment (TTRA) serves as the basis of CI analysis of foreign intelligence entity threats against a program and is a key element of the program protection plan (PPP), which is also required for every major milestone decision.[23]

---

[19] Acquisition Intelligence Formal Training Unit, Wright-Patterson Air Force Base, December 2019.

[20] DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*, Washington, D.C.: U.S. Department of Defense, January 22, 2013, Incorporating Change 1, August 29, 2017.

[21] "Validated intelligence" indicates that threat assessments use appropriate and complete intelligence, are consistent with existing intelligence positions, and use accepted analytic tradecraft in their development assessments. DIA validation means that the intelligence product as written addresses the question and is of appropriate scope, but is not a substantive validation. DIAI 5000.002, 2013.

[22] DIAI 5000.002, 2013.

[23] DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, Washington, D.C., U.S. Department of Defense, June 8, 2011, Incorporating Change 1, Effective October 15, 2013. Not available to the general public.

As part of the VOLT production process, program offices, in collaboration with the primary supporting service intelligence center, should develop CIPs that "clearly define the performance threshold at which a foreign system may compromise mission effectiveness of the U.S. system."[24] CIPs are included for capabilities in development that are deemed threat-sensitive. When a program determines that a CIP is warranted, it will submit a comment and supporting rationale to the requirement sponsor for adjudication during JCIDS staffing.

Most intelligence threat-assessment production requirements reside at service intelligence centers while DIA validates the final product. For DAF, most programs require intelligence assessments from documents such as VOLT to come from NASIC. Air Force Mission Directive 24, *National Air and Space Intelligence Center (NASIC)*, identifies the organization's mission: "to create integrated predictive intelligence in the Air, Space, and Cyberspace domains, to enable military operations, force modernization and policy making."[25] Oblique references to acquisition and requirements communities come through mention of "force modernization," "having functional expertise on S&TI[scientific and technical intelligence]," and "provid[ing] robust, enduring, and focused foundational intelligence analysis products and services in direct support of stated requirements from AF major commands."[26]

The focus of intelligence policy and guidance documents on internal policies often fails to identify specific points of contact for midlevel intelligence analysts and acquisition officials. For example, documents often neglect to mention the specific part of an organization a member of the acquisition or requirements community should contact for intelligence support, except in limited references, such as DIA and its TLA office for coordinating VOLTs and CIPs.[27] For intelligence, these documents also fail to identify how analysts link up with program offices or contact requirements holders to provide analytic support; this dem-

---

[24] DIAI 5000.002, 2013.

[25] AFMD 24, *National Air and Space Intelligence Center (NASIC)*, U.S. Department of the Air Force, September 22, 2016, p. 1.

[26] AFMD 24, 2016.

[27] DIAI 5000.002, 2013.

onstrates the imbalance in the "push/pull" relationship between these communities. Conversely, DoD CI documents not only establish procedures for requesting and producing CI assessments supporting the DAS, but also identify specific points of contact for PEOs and PMs to request such material. For DAF programs, supply-chain risk management (SCRM) and TTRA support come through AFOSI due to that organization's writ to support and conduct CI investigations. At the DoD level, however, DIA also plays a role in CI and supply-chain threat assessments.[28]

Counterintelligence Responsibilities

As in the other services, DAF CI investigations and assessments regarding threats to the supply chain reside with AFOSI. NASIC or MAJCOM A2s must coordinate with AFOSI on any related threats in this realm resulting from separation between intelligence and law enforcement responsibilities and concerns regarding perceptions of intelligence investigating U.S. persons and companies.[29] As a law enforcement agency, AFOSI investigates illegal and criminal activity and intelligence threats that undermine the mission of the Air Force; these threats include acquisition fraud, potential challenges in the supply chains, or corruption in the contracting process.[30] CI capabilities, however, also reside in-house at DIA. DIA CI responsibilities for acquisitions include validation and possible production of VOLT reports, TTRA, SCRM, PPPs, and any CI assessments required for CIPs; these responsibilities fit with DIA's mission to conduct CI analy-

---

[28] DIAI 5000.002, 2013.

[29] AFMAN 14-401, 2019; AFPAM 63-113, *Program Protection Planning for Life-Cycle Management*, U.S. Department of the Air Force, October 17, 2013; DoDI O-5240.24, 2013. Not available to the general public; DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, Washington, D.C., U.S. Department of Defense, Incorporating Change 2, August 8, 2016, governs DIE restrictions related to collection on U.S. persons. DIE includes DoD intelligence, counterintelligence, and security communities; see Grant Schneider, *DS Strategic Vision 2012–2017*, Washington, D.C.: Defense Intelligence Agency, 2012.

[30] U.S. Department of the Air Force, "Air Force Office of Special Investigations: Fact Sheet," April 15, 2005.

sis of foreign-intelligence entity threats.[31] The separation of CI analysis from NASIC and A/2s could prevent holistic, life-cycle intelligence support, leading to gaps and potentially curtailing collaboration on threat assessments. Indeed, most interviews uncovered the fact that the critical role of CI in the DAS was barely recognized.

Impact on Intelligence Support of Updating Acquisition Processes

When considering policies, intelligence remains a supporting element to both the requirements and acquisition communities, and this has placed intelligence in a position of primarily responding to both communities. Intelligence policies at the DoD, Combat Support Agency, and DAF levels reflect this reactive nature of intelligence support. With increased recognition of the importance of threat-informed acquisition, however, the IC will need to become a more active participant in the acquisition life cycle, including the requirements phase. Often, the IC has a seat at the table (e.g., USD[I&S]) and is a formal adviser to the Joint Requirements Oversight Council [JROC]),[32] but perhaps the IC should take a more active role in leveraging these participatory avenues. Inclusion of intelligence at the requirements phase, however, does not provide full representation and inclusion of the IC since USD(I&S) is not a production organization. Therefore, it may not have the resources or expertise to represent substantive intelligence issues at this high-level forum unless the issues are already known and are a source of contention between the IC and the acquisition community.

A critical point to highlight is that current intelligence policies for the DAS are focused on supporting the current ACAT structure and on the largest programs designated as MDAPs and their milestones.[33] While resources and processes designed for ACAT 1D programs can be used for smaller programs or smaller programs can request analyses specifically for them, these are not perfect fits. With ACAT 1 programs receiving prioritization, programs at lower ACAT levels may not get

[31] DIAI 5000.002, 2013.

[32] As per 10 U.S.C. 181(d)(1)(B), Joint Requirements Oversight Council, December 20, 2019.

[33] DoDI 5000.02, 2018; DoDD 5105.21, 2008.

the specific collection or production priority necessary for them, so the resulting intelligence information, analysis, and products will not be of as great a value. Intelligence support and policies will likely have to adapt as DoD and DAF continue to move toward more agile acquisition processes. The updated version of DoDD 5000.01, published on September 9, 2020, will likely have a cascading effect on all other guidance documents discussed in this chapter, including intelligence documents that refer to DoDD 5000.01.

Policy Review Through the Requirements Lens

While JCIDS recognizes the criticality of intelligence and defines processes and documents to that end, at the same time, it denies intelligence a co-equal partnership with requirements, acquisition, and budgeting. Intelligence input is involved in informing the generation or amendment of requirements, which is rooted in official documentation. While there is ample guidance on what sort of intelligence should be included in critical requirements documents and at key milestones, the requirements documentation at both the JCIDS and Air Force levels does not appear to be flexible with regard to when intelligence enters the process. In addition, the guidance documents are inconsistent in terms of how much a program should consider intelligence and threat information in critical decisions. Despite acknowledging that key parameters could shift over the life cycle of the project or capability, existing policy does not make room for ad hoc intelligence input and subsumes potential impacts from the IC as another type of cost to address rather than an independent factor that might guide both capability design and evolution. These issues reinforce the DAS process remaining capabilities-based, rather than threat-based.

The Joint Capabilities Integration and Development System

JCIDS provides the overarching framework for requirements development, the baseline for documentation, review, and validation of

capability requirements across DoD.[34] Through JCIDS, new potential solutions undergo a capability and gap analysis that informs the memorialization of requirements for both materiel and nonmateriel solutions, which in turn feed requirements for the acquisition process.[35] The JCIDS manual describes intelligence activities as follows:

> Intelligence activities identify and quantify threats that may drive or impact military operations, and the level of effectiveness needed to perform tasks, thus inform[ing] the setting of performance levels in capability requirements. The need to collect intelligence also drives capability requirements, often worked collaboratively between military and intelligence requirements processes when there are shared equities in the intelligence gathering capabilities.[36]

JCIDS mandates the production of several documents that identify gaps and establish performance attributes. These documents are key components of a materiel solution's progress through major acquisition and requirements milestones. ICD identifies capability requirements and potential gaps, driving the development of solutions (whether materiel, nonmateriel, or a combination thereof). This document typically leads to an analysis of alternatives (AoA) and then either a CDD for development of a materiel or nonmateriel solution.[37]

A validated ICD (the result of a capabilities-based analysis or other study) informs a materiel development decision (MDD), the material solution analysis (MSA) phase, and the conduct of an AoA. By Milestone A, a draft CDD has been approved by the sponsor but has not yet been submitted for Joint Staff approval. By Milestone B, CDD is validated prior to entering the engineering and manufacturing development phase. In preparation for Milestone C, CDD might

---

[34] Patrick Willis, "Joint Capabilities Integration and Development System (JCIDS): A Primer," Defense Acquisition University, January 31, 2019, p. 6.

[35] Willis, 2019, pp. 7–8.

[36] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. C-5.

[37] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. A-A-8.

receive further updates and validation. Intelligence inputs or a review are required at each milestone.

Complementing the intelligence inputs to documents for each milestone, national-level intelligence agencies—DIA, NGA, and the National Security Agency (NSA)—also play a role in supporting the JCIDS process.[38] Each of these organizations is also designated as a combat support agency by DoD and is charged with helping to define and validate future joint warfighting capability needs through JCIDS (whether for themselves as part of their supporting role or with respect to joint capabilities and relevant shortfalls).[39]

NGA and NSA roles in the JCIDS process relate to their agency-specific capabilities and skills. DIA, however, plays a larger role in coordinating the intelligence threat-assessment process and providing intelligence support and advice to JROC on adversary capabilities. DIA is also responsible for ensuring that its appropriate organizational components review capability-requirements documents according to the following criteria:

- threat information and use of current DIA- or service-approved threat products
- intelligence support and intelligence-related operational requirements for completeness, supportability, potential shortfalls, and impact on intelligence strategy, policy, and architecture planning
- IMD requirements identifying production or sharing opportunities across acquisition programs and operational systems and providing an assessment of IMD availability to support program IMD needs
- CI support requirements, identifying intelligence threat-assessment production requirements to support program-specific CI needs

---

[38] Chairman of the Joint Chiefs of Staff Instruction 5123.01H, *Charter of the Joint Requirements Oversight (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS),* August 31, 2018, p. B-17.

[39] DoDD 3000.06, *Combat Support Agencies (CSAs)*, Washington, D.C.: U.S. Department of Defense, June 27, 2013, pp. 2, 9.

- intelligence network support and interoperability requirements and information assurance and information security protocols.[40]

Even though JCIDS lays out these specific roles for DIE, much of the responsibility for developing requirements lies with requirements sponsors. When identifying capability requirements, sponsors "use certified requirements managers to monitor and evaluate capability requirement identification, including but not limited to the identification of capability gaps due to changes in threats, missions, or aging of legacy weapon systems throughout their life-cycle."[41] Notably, the list of suggested approaches to identifying capability requirements in the JCIDS manual does not explicitly include intelligence or threat information, apart from the general need to assess capability gaps.[42] This does not mean, however, that intelligence is ignored; in other places the JCIDS Manual explicitly states the importance of intelligence in DOTMLPF-P change recommendation and system requirements.[43] Requirements sponsors are responsible for establishing performance attributes that are "technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E."[44]

Intelligence supportability and certification receive substantial attention in JCIDS. The objective of intelligence supportability is to

> ensure that capability solutions are developed in the context of applicable adversary threat capabilities, that intelligence requirements have been identified and documented at the earliest possible point, and that all likely intelligence support requirements

[40] Chairman of the Joint Chiefs of Staff Instruction 5123.01H, 2018, pp. C-24, C-25.

[41] Willis, 2019, p. 18.

[42] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. C-B-2.

[43] See, for example, Chairman of the Joint Chiefs of Staff Instruction J8, 2018, pp. B-E-4, C-5, C-10, and GL-16.

[44] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. B-G-1.

> and shortfalls (if applicable) have been assessed for availability, suitability, and sufficiency.[45]

The scope of intelligence certification, which ultimately determines intelligence supportability, includes the entire program or capability life cycle and seeks to ensure that sponsors have integrated the most current and applicable intelligence into their capability development efforts, so that the architecture can continue to support future warfighting while precluding the fielding of capabilities that the national and defense intelligence communities cannot sustain.[46]

Intelligence supportability content is an input to ICDs and CDDs. For an ICD, in addition to the threat summary and CIP information, sponsors must also identify the known and applicable intelligence support categories in the capability requirements and gaps and overlays sections of ICD (including a description of the intelligence support requirements, resources, or other programs necessary to enable each capability, and any current or projected gaps or shortfalls in intelligence support related to a category). In CDD, the sponsor must include a paragraph on intelligence supportability that covers all intelligence support requirements and anticipated shortfalls throughout the solution's life cycle in the following areas: staffing, funding, planning and operations, interoperability, targeting, mission data, space, CI, and training.[47]

Intelligence certification, including the DIA TLA office's threat approval, IMD evaluation, and when applicable, the DIA Directorate for Operations Office of Counterintelligence protection threat review and threat production validation, pertains to all requirements. Sponsors are required to provide enough information and perform adequate analysis so that reviewers can assess both requirements and shortfalls. The IC might find either that it cannot meet the capability's intelligence support requirements or that the capability itself creates an intelligence shortfall. Certification is contingent on a full articulation of the

---

[45] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. B-G-G-1.

[46] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. B-G-G-1.

[47] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. B-G-G-6.

threat and intelligence support requirements as well as threat approval from DIA.[48] Intelligence certification accompanies each stage of the requirements process.

Air Force Requirements Documents

DAF has its own analogous set of requirements development guidelines and responsibilities, which mirror those outlined in JCIDS. CSAF is designated as the Air Force Chief Requirements Officer. The Deputy Chief of Staff, Strategy, Integration and Requirements, AF/A5 (through AF/A5R) is the office of primary responsibility (OPR) for implementation of DAF operational capability requirements development, as described in HAF Mission Directive 1-7.[49] Sponsorship is assigned to a MAJCOM or agency to lead the development of capability requirements and associated documentation for their assigned systems, programs, functions, or missions. Sponsorship includes, but is not limited to, advocating for resourcing, staffing, and any other support necessary for requirements development activities.[50]

The Air Force lead for intelligence is the Deputy Chief of Staff for ISR and Cyber Effect Operations (AF/A2/6).[51] AF/A2/6 has the following functional areas of responsibility: integration and oversight of Air Force ISR and Information dominance mission area capabilities; oversight and direction of SMEs for intelligence supportability, IMD, and CIPs; and liaison with Joint Staff J2 and DIA for threat and intelligence certifications.[52] More specifically, AF/A2/6 is charged with (1) providing policies and guidance relative to intelligence support to acquisition; (2) ensuring intelligence issues are addressed; (3) ensuring sufficient analysis has gone into the required milestone documents;

---

[48] Chairman of the Joint Chiefs of Staff Instruction J8, 2018, p. B-G-G-2.

[49] U.S. Department of the Air Force, *AF/A5R Requirements Development Guidebook, Volume 1: Guidelines, Oversight and Governance*, Air Force Requirements Integration Division, Washington, D.C., December 5, 2019b, p. 8.

[50] U.S. Department of the Air Force, 2019b, p. 8.

[51] U.S. Department of the Air Force, 2019b, p. 9.

[52] U.S. Department of the Air Force, 2019b, p. 22.

and (4) facilitating the relationships among the programs, Air Force intelligence, and the IC.[53]

The implementing command, whether AFMC, AFSPC, or Air Force Civil Engineering Center (AFCEC)), assists Air Force acquisition program offices with intelligence-sensitive programs in defining, documenting, and resolving relevant threat, intelligence supportability, and infrastructure requirements to support operational system development, test and evaluation, and acquisition. The implementing command also provides intelligence health assessments to AF/A2 to support JCIDS intelligence certification process.[54] AF/A2/6 is critical for ensuring guidance and policy; however, intelligence assets at the implementing commands and program offices remain the primary support mechanisms for the DAS.

Air Force Acquisition and Requirements

Despite JCIDS's efforts to include intelligence and to be threat-informed, neither is consistently carried down into or prioritized by the services, including the Air Force. According to the Air Force's instruction for operational capability requirements development,

> Air Force requirements are driven by *desired effects and needed capabilities*. All stakeholders in the acquisition framework must know why the Air Force needs a capability, how and where it will be used, who will use it, when it is needed, and how it will be supported and maintained. For a materiel solution, fielding an operational system starts with sound strategies for concept refinement, requirements development, acquisition and sustainment life-cycle management, and test and evaluation (T&E). *To be viable, these strategies must be developed in concert and require early and ongoing collaboration among operators, developers, programmers, systems engineers, acquirers, testers, sustainers, and intelligence analysts*.[55]

---

[53] AFI 10-601, *Operational Capability Requirements Development*, U.S. Department of the Air Force, November 6, 2013, p. 3.

[54] AFI 10-601, 2013, p. 25.

[55] AFI 10-601, 2013, pp. 9–10; emphasis added.

While intelligence analysts are included on this list, our interviewees indicated that the list appears to be in a general priority order. Intelligence analysts are inconsistently included in early discussions and often have to push to be included in collaborative efforts, especially if they are not co-located with requirements or program offices.

For intelligence-sensitive programs, the sponsoring MAJCOM or agency is supposed to coordinate with the supporting intelligence representatives to detail the future threat environment and assess the extent of intelligence supportability, mission data, and infrastructure support that is necessary for the capability to be fully fielded, supported, and sustained.[56] Despite the inclusion of this language, DAF's diagramming of the capabilities requirements process does not call out intelligence as a factor in generating or selecting solution approaches; only after selection does there appear to be a formal role for intelligence systems and services.[57] While elements of the process include intelligence analysis as foundational information, such as a comparison between mission needs and forces, some interviewees raised the concern that the IC is often consulted only at a cursory level. At the same time, the requirements guidelines do not expect capability requirements to be static during the product life cycle and anticipate that changes to performance attributes, cost, schedule, or quantity, but not the operational threat environment, could occur.[58] Similarly, although CIPs are established to alert programs to changes that "could critically impact the effectiveness and survivability of the proposed system,"[59] many of those we spoke with in program offices indicated that, when presented with a CIP breach, PMs took risks rather than addressing the issue because costs would rise or schedules would be delayed. Moreover, not all programs have CIPs.

DAF's Requirements Development Guidebook lists the key tenets of Air Force capability requirements development as stability, affordabil-

---

[56] U.S. Department of the Air Force, 2019b, p. 21.

[57] U.S. Department of the Air Force, 2019b, p. 14.

[58] U.S. Department of the Air Force, 2019b, p. 20; AFPD 10-6, *Capability Requirements Development*, U.S. Department of the Air Force, November 6, 2013, p. 2.

[59] DIAI 5000.002, 2013.

ity, timeliness, and feasibility in a way that ties into the cost-schedule-performance mindset of the DAS. These tenets do not explicitly include a role for intelligence.[60] DAF's concept of integrated life-cycle management encompasses development planning and early systems engineering, intelligence support considerations, materiel cost-effective prioritization, and evolutionary acquisition. On intelligence support, it states:

> Most warfighting weapon systems require intelligence inputs to include threat and mission data. Intelligence specialists provide the necessary interface to the national Intelligence Community (IC) with which to access intelligence data and to enter into formal IC production requirements and planning processes. Not all requirements for intelligence data are supportable, in which case intelligence must be considered from a cost/capability perspective. Early collaboration between Requirements, Acquisition, and Intelligence communities is critical to ensuring decisions regarding desired materiel solutions fully account for capability impacts presented by intelligence dependencies.[61]

Here, intelligence and threat considerations are subsumed under cost and capability.

At the same time, intelligence supportability does appear in Air Force documentation as part of each milestone review. The AoA study plan includes the identification of OPRs for intelligence supportability.[62] For the draft (Milestone A) and final CDD (Milestone B) to be approved, the Air Force Requirements Review Group (AFRRG) and Air Force Requirements Oversight Council (AFROC) are to review intelligence supportability requirements.[63] The capabilities production document at Milestone C is also supposed to include an AFFRG and AFROC review of intelligence supportability requirements.[64] Beyond

[60] U.S. Department of the Air Force, 2019b, pp. 11–12.

[61] AFI 10-601, 2013, p. 11.

[62] AFI 10-601, 2013, p. 41.

[63] AFI 10-601, 2013, pp. 45, 47.

[64] AFI 10-601, 2013, pp. 48–49.

these official documents, however, there is less room for intelligence to influence the requirements and acquisition processes. Despite recognizing that key parameters can shift over the life cycle of the project or capability, existing requirements policy does not make explicit room for ad hoc intelligence input and subsumes potential impacts from intelligence as another type of cost to address rather than an independent factor that might guide both capability design and evolution. Though directed at an important goal—making policy simple and flexible while encouraging acquisition personnel to think critically about more tailored solutions—many in the program offices where we interviewed indicated that in practice they did not reach out proactively for intelligence support and did not display a willingness to "absorb the programmatic impacts [from intelligence] in the resources that they had."[65] By contrast, as one acquisition intelligence official told us, programs want to "run free" and avoid intelligence injects that "slow programs down, make [the] system seem obsolete, or can significantly increase program cost."[66]

Policy Review Through the Lens of the Defense Acquisition System

Overall, the DAS requires intelligence support in four distinct areas: (1) intelligence sensitivity and supportability analyses, (2) forecasts of adversary threat trends, (3) operational threat scenario development, and (4) CI information. PMs play a primary role, along with oversight managers and the requirements community, in deciding the level of IC involvement in the execution of the acquisition program, especially as it pertains to PPP.[67] PMs determine overall program protection requirements and updates the program protection plan based on recent threat data, among other reasons.[68] The IC serves as sup-

[65] Interview at SMC, April 2020.

[66] Interview at AFMC/A2, April 2020.

[67] The term "intelligence community" includes DIE.

[68] AFPAM 63-113, 2013, p. 28.

port activity to ongoing acquisition program execution. Intelligence representatives working with acquisition programs forecast military technology of threat countries so that DAF programs can develop countermeasures. These representatives also provide intelligence on the current state of foreign technologies and predictive intelligence on foreign cyber capabilities and intent.[69]

Areas of Intelligence Supporting the Defense Acquisition System

Intelligence sensitivity and supportability analyses help to identify programs that are dependent on IMD and require monitoring and reporting on CIP breaches. Forecasting adversary threat trends encompasses the creation of VOLT reports, which project technology and adversary capability trends for the following 20 years, analysis of threats in response to requests for information (RFIs), assessments of the current state of foreign technologies, forecasts of military technology needs of threat countries, and predictive intelligence on foreign cyber capabilities and intent.[70] Predictive intelligence assessments, however, are of most value in the early stages of the acquisition process as threat projections and other key elements inform analysis of alternatives during the MSA phase.[71]

The IC also supports operational threat scenario development by providing validated threat data for M&S during testing, by validating any new threat environments that might have an impact on weapon system operational effectiveness, and by collecting combat damage data to enhance weapon system survivability and readiness. Intelligence

---

[69] DoDI 5000.02T, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015, Incorporating Change 3, August 10, 2017. Note that DoDI 5000.02, 2020, will eventually replace the DoDI 5000.02, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015 version. The January 2015 version has been renamed DoDI 5000.02T (Transition) to establish a distinction between the two issuances.

[70] See, for example, U.S. Department of the Air Force, "Air Force Doctrine Publication 2-0 - Global Integrated ISR Operations," January 29, 2015.

[71] DoDI 5000.02T, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015, Incorporating Change 9, November 19, 2020, p. 19.

products such as the VOLT assessment are also used to support testing in a relevant operational threat environment at the time of program execution. Finally, DAF and DoD CI entities provide CI information to protect critical program information (CPI) and critical components with TTRAs, CI threat assessments, assessments of supplier threats to acquisition programs (e.g., threat analysis of critical component suppliers), analysis of suspicious contacts or activities occurring within the defense contractor community, and anti-tamper support requirements.

The effect of the operational environment becomes evident during testing. The IC employs VOLT scenarios to support developmental and operational testing and evaluation (DT&E, OT&E) activities with threat appropriate Red Team and cybersecurity T&E.[72] The Milestone Decision Authority considers any new validated threat environments that might impact weapon system operational effectiveness before making full-rate production and deployment decisions.[73] Evolving threats might also warrant revisions to the life-cycle sustainment plan (LCSP) for operations and sustainment considerations.[74]

Threat projections also include threats from foreign intelligence entities (FIE) and support development of PPPs. PPP requires assessment and identification of threats to and vulnerabilities of CPI and critical components through application of CI, intelligence, security, systems engineering, information assurance, anti-tamper, and other defense countermeasures to mitigate threats posed by FIE.[75] The IC works with CI entities to support the PM with formal threat reports, supply-chain threat assessments, and other threat documents, as well as a listing of identified threats mandated in PPP.[76] The specific FIE threats include collection; tampering activities in the event of battle-

[72] DoDI 5000.02T, 2020, p. 30.

[73] DoDI 5000.02T, 2020, p. 31.

[74] DoDI 5000.02T, 2020, p. 32.

[75] AFPAM, 2013.

[76] DoD, "Program Protection Plan Outline & Guidance, Version 1.0," Washington, D.C., Deputy Assistant Secretary of Defense Systems Engineering, July 2011.

field loss; and exploitation of hardware, software, supply chain, and cybersecurity during the program's life cycle.[77]

Cybersecurity and the Defense Acquisition System

The importance of cybersecurity in acquisition programs is evident in the emphasis applied to cybersecurity management procedures in the DAS, especially with respect to the PM's interaction with intelligence support at each acquisition phase. Cybersecurity is a requirement for all DoD programs and must be "considered and implemented in all aspects of acquisition programs across the life cycle."[78] As the PM aims to implement cybersecurity and related program security across the program's life cycle to reduce the risk associated with cyberattacks by state and nonstate actors, he or she closely interacts with intelligence organizations to request formal and informal support in order to develop and deliver a system that can survive these threats. The PM's involvement with intelligence support begins prior to MDDs and continues through operations and sustainment. Table 3.1 summarizes the PM and component actions' step-by-step interaction with intelligence support to implement cybersecurity and related program security across the materiel life cycle. The table also lists selected examples of actions the responsible authorities will undertake in response to or supported by the provided intelligence.

The PM's interactions with intelligence activities to implement cybersecurity protections for the program outline how threat informa-

---

[77] Several policies contribute to the requirements stated in the Program Protection Planning. Examples include DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E),* Washington, D.C., U.S. Department of Defense, May 28, 2017, Incorporating Change 1, November 17, 2017; DoDD 5200.47E, *Anti-Tamper (AT),* Washington, D.C.: U.S. Department of Defense, September 4, 2015, Incorporating Change 2, August 31, 2018; DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),* Washington, D.C., U.S. Department of Defense, November 5, 2012, Incorporating Change 2, July 27, 2017; and DoDI 8500.01, *Cybersecurity*, Washington, D.C., U.S. Department of Defense, March 14, 2014, Incorporating Change 1, October 7, 2019.

[78] DoDI 5000.02T, 2020, Enclosure 14, "Cybersecurity in the Defense Acquisition System," p. 155. (Note: DoDI 5000.CS "Cybersecurity for Acquisition Decision Authorities and Program Managers" is under development and will eventually replace Enclosure 14.)

Table 3.1
Project Manager Interaction with Intelligence Support on Cybersecurity

Acquisition Cycle Phases	Responsible Authority	Interaction with Intelligence Support	Example Actions Based on Provided Intelligence Support
Before Materiel Development Decisions	All Research, development, test and evaluation (RDT&E) organizations, PM	Request cyber threat information from DIA or DoD Component intelligence/counter-intelligence activities and use threat assessments to inform cyber protection planning	Support requirements community in identifying critical intelligence parameters Protect digitized information from adversary targeting during basic and applied research, advanced technology development (including technology demonstrations and prototyping), and capabilities-based assessments
MSA Phase	RDT&E organizations, PM	Request cyber threat information targeting program information and system from DIA or DoD Component intelligence/counter-intelligence activities and use updated threat assessments to inform AoA, systems engineering analyses, selection of preferred materiel solution, and development of draft Capabilities Development Document (CDD)	Ensure key system elements/interfaces identified through criticality and vulnerability analyses are tested during T&E Establish program and system cybersecurity and related program security metrics and implement an enduring monitoring and assessment capability
Technology Maturation and Risk Reduction (TMRR) Phase	PM	Request cyber threat information from DIA or DoD component intelligence/counter-intelligence activities and use updated threat assessments to inform systems engineering trade-off analyses to support requirements/investment/acquisition decisions	Ensure adversarial cybersecurity developmental testing and evaluation (DT&E) event is planned in mission context Protect digitized program and system information, CPI, and other system elements from adversary targeting during TMRR activities, including system definition, design and test, contracting, and competitive prototyping

Table 3.1—Continued

Acquisition Cycle Phases	Responsible Authority	Interaction with Intelligence Support	Example Actions Based on Provided Intelligence Support
Engineering and Manufacturing Development	PM	Request cyber threat information targeting program information and system from DIA or DoD Component intelligence/counter-intelligence activities and use updated threat assessments to inform development of detailed design, T&E criteria, system-level security risk, and assessment of readiness to begin production/deployment	Use realistic threat exploitation techniques in representative operating environments/scenarios Protect digitized program, system, and test information, CPI, and system elements from adversary targeting during design, test, and manufacturing and production readiness
Production and Deployment	PM	Request cyber threat information targeting program information and system from DIA or DoD component intelligence/counter-intelligence activities and use updated threat assessments to inform production/deployment activities such as manufacturing, and training spares	Test system for cybersecurity vulnerabilities using realistic threat exploitation techniques in operational environment Protect digitized program and system information, CPI, and the system from adversary targeting during initial production, operational T&E, and initial fielding
Operations and Support	PM	Request cyber threat information targeting program information and system from DIA or DoD component intelligence/counter-intelligence activities and use updated threat assessments to inform impact to operational systems, technology refresh, and disposal plans	Update all aspects of program protection planning for program/system as cyber threats/systems evolve Protect digitized program and system information, CPI, and system from adversary targeting during fielding and sustainment activities such as maintenance, training and operational exercises

SOURCE: DoDI 5000.02T, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015, Incorporating Change 9, November 19, 2020, pp. 164–168.

tion affects acquisition processes, program procedures, activities, and documentation at every phase of the program, as well as align the specific acquisition activities with the associated intelligence activities that must occur at each phase of the program.[79] This is a good example of the close and continuous relationship between acquisition and intelligence entities throughout a program's life cycle, as well as an illustration of how and where the provided intelligence can be applied in a given acquisition program.

The Adaptive Acquisition Framework

In general, intelligence support is recognized as integral to the development and delivery of secure, operationally effective capabilities.[80] DAS also recognizes that system performance must be confirmed against documented adversary capabilities as described in the system threat assessment.[81] However, DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, notes that DoD component heads "are responsible for aligning the management of acquisition programs with three principal DoD processes," which include JCIDS, PPBE, and DAS, as the new *Air Force Guidance Memorandum for Rapid Acquisition Activities* lists capability requirements, financial, T&E, and operations as the key stakeholders in rapid acquisition activities.[82] While the DAS recognizes the importance of intelligence support to acquisition processes, neither set of the aforementioned relationships formally includes the IC. If the DAS is to respond more efficiently to the 2018 NDS call for intelligence-driven acquisition processes, it might be useful to mention the IC more often as one of the critical members of these kinds of groups.

Under SAF/AQ's push to shorten acquisition (in part by using the Adaptive Acquisition Framework and in particular the middle-tier pathway), it is likely that fewer future DAF acquisition programs will

---

[79] DoDI 5000.02T, 2020, pp. 164–168.

[80] DoDD 5000.01, 2020.

[81] DoDD 5000.01, 2020, p. 8.

[82] DoDD 5000.01, 2020, p. 7; U.S. Department of the Air Force, *Air Force Guidance Memorandum for Rapid Acquisition Activities*, 63-01, June 27, 2019a, p. 3.

be classified as MDAPs, and thus fewer programs will be subject to the JCIDS process and oversight and the DAS directive DoDD 5000.01.[83] The new rapid acquisition approach calls for completion of all *statutory* requirements and of *regulatory* requirements as applicable to their specific rapid acquisition authority (e.g., Rapid Prototyping, Rapid Fielding).[84] The operation of the DAS levies *statutory* and *regulatory* milestone and phase information requirements on each program to complete.[85] Unlike *statutory* requirements, the *regulatory* requirements can be "tailored-in" or waived based on program needs.[86] The Cybersecurity Annex to PPP, for example, is a *statutory* requirement, yet the PPP itself is a *regulatory* requirement that could be tailored or waived.[87]

Because intelligence data and threat information requirements are all *regulatory* and apply only to MDAPs, major acquisition information systems, and programs in ACAT II and below III, PMs (with the support of MDA) will be able to consider the intent of intelligence documents that address program protection of CPI, supply-chain risk, and anti-tamper considerations, as well as intelligence and threat information and life-cycle mission data plan and complete only those that are applicable.[88] This means that PMs may be requesting fewer planned or foundational intelligence products from the IC.

---

[83] 10 U.S.C. 2430(a)(2)(A), Major Defense Acquisition Program Defined, January 24, 2020; Public Law 114-92, National Defense Authorization Act of Fiscal Year 2016, Section 804; DoD, "Middle Tier of Acquisition (Rapid Prototyping/Rapid Fielding) Interim Authority and Guidance," Washington, D.C., Under Secretary of Defense for Acquisition and Sustainment, April 16, 2018b; DoDI 5000.80, *Operation of the Middle Tier of Acquisition (MTA),* Washington, D.C., U.S. Department of Defense, December 30, 2019, p. 4; DoDI 5000.02, 2020; DoDD 5000.01, 2020, p. 7; U.S. Department of the Air Force, 2019a, p. 1.

[84] U.S. Department of the Air Force, 2019a, p. 8.

[85] DAU, "Milestone Document Identification: The DoD Information and Reporting Requirements Tool," undated(b).

[86] DoDD 5000.01, 2020, p. 6.

[87] DAU, undated(b).

[88] Intelligence data includes the information requirement for the Life-Cycle Mission Data Plan, threat information includes information requirements for the VOLT Report, Threat Summary for ICD, and TTRA; U.S. Department of the Air Force, 2019a, p. 8.

Intelligence Breaches Versus Cost-Related Program Breaches

DAS realizes that threats are not static and must be identified and monitored throughout a program's life cycle. A significant challenge for PMs is to balance program costs, schedule, performance, and threat information—especially as the latter comes from many different sources across national, defense, and service-level intelligence organizations—in order to address as many program vulnerabilities as possible—such as threats to the supply chain and cybersecurity, as well as anti-tamper activities—given limited resources and trade-offs.

One manifestation of this challenge is in the different ways that programs respond to CIP breaches versus Nunn-McCurdy breaches, which require that DoD report to Congress when programs experience certain levels of cost growth above the baseline.[89,90] The latter requires notification to Congress for all MDAPs that experience cost overruns that exceed certain thresholds, while the former requires notification to the PEO, MDA, and the implementing command's intelligence focal point for any program for which a foreign system has met a CIP threshold.[91] Following a CIP breach notification, the Configuration Steering Board determines the need for any further action.[92] A CIP breach could call for a program to make adjustments, modifications, activate risk-mitigation protocols, or re-baseline. "Changes that increase cost will not normally be approved unless funds are identified and schedule impacts are addressed."[93] CIP breaches could lead to Nunn-McCurdy breaches, but congressional policy response skews toward the latter in

---

[89] CIPs define the threshold at which the performance of a foreign system or capability could compromise the program or mission effectiveness of the AFI 63-101/20-101, *Integrated Life-Cycle Management*, U.S. Department of the Air Force, May 9, 2017, p. 51.

[90] Nunn-McCurdy breaches are defined in law in 10 U.S.C. 2433a, Critical Cost Growth in Major Defense Acquisition Programs, January 24, 2020.

[91] AFI 63-101/20-101, 2017; DoDI 5000.02, 2020; 10 U.S.C. 2433a.

[92] This board reviews requirements and technical configuration changes that may result in cost and schedule impacts to the program, AFI 63-101/20-101, 2017, p. 26; DoDI 5000.85, 2020, p. 33.

[93] DoDI 5000.85, 2020, p. 33.

that automatic triggers are set up for cost and schedule but less for system performance against evolving threats.

Additionally, the law specifies that the Secretary of Defense shall terminate an MDAP as a result of a Nunn-McCurdy breach unless a written certification is provided within a prescribed time that this MDAP is essential to national security, is the only acceptable capability to meet the joint military requirement, has reasonable new acquisition and procurement unit cost estimates, is higher priority than other programs whose funding must be reduced to accommodate the growth in cost of this MDAP, and has an adequate program management structure to manage and control future program costs.[94] MDA can also decide to terminate a rapid prototyping action if it does not meet the criteria for subsequent prototyping, initiation of rapid fielding, transition to a traditional program, or inclusion in an existing program.[95] Policy response to terminate a program due to a CIP breach or insufficient intelligence data or threat information is less prescribed and thus subject to leadership decisionmaking. This flexibility is not necessarily bad because it allows DAF to consider a wide range of factors and options tailored to each situation while reducing the bureaucratic requirements of events such as a Nunn-McCurdy breach. On the other hand, this means that CIP breaches might get lower-priority consideration to avoid cost increases.[96]

Implications of Agility for Intelligence Support

In summary, the push to create more agility in the DAS, the differences between regulatory and statutory milestone and phase information requirements, and the individual programmatic decisions that PMs and MDA make regarding applicability of those information requirements to specific acquisition authorities result in differing levels of prescribed intelligence support across defense acquisition programs. Additionally, the DAS focus on agility in the adaptive framework and DAF's focus on more rapid acquisition through extensive use of middle-tier acquisi-

[94] 10 U.S.C. 2433a.

[95] U.S. Department of the Air Force, 2019a, p. 5.

[96] Interview with AFMC/A2, April 2020.

tion, which resulted from authorities granted to DoD in 2016, reflect the intent of fielding weapon systems faster so as to ensure warfighter competitive advantages by proactively leveraging disruptive technologies and addressing operational environment changes. Going forward, the IC's role in the acquisition processes could change, depending on the chosen pathway, and the DAS could expect a quicker reaction from its intelligence support than before. There may be barriers, however, to the effective use of the IC to inform acquisitions. For example, in 2019, GAO found that two defense intelligence production centers could not respond to the Missile Defense Agency's request for an accelerated schedule "due to their manpower and resource levels."[97] This agency also exercises acquisition flexibilities under which it is not required to engage DIE on how to design and test weapon systems and provides GAO limited insight into how it uses threat assessments to inform its acquisition decisions.[98] The GAO report concluded that gaps in coordination with DIE "can have significant implications on the performance of [the agency's] weapon systems."[99]

Interviewees' Perspectives on Policy and Implementation

Our interviews revealed varied perspectives on existing the DAS policies for integrating intelligence information. Interviewees generally agreed that the DAS policy clearly outlines the responsibilities of the acquisition managers with regard to what they need from DIE (e.g., products they need to drive acquisition processes). Some, however, expressed the desire for policy to be more flexible with regard to what type of support acquisition programs need to seek from DIE. For example, continuous threat updates might be more useful than the required VOLT.

---

[97] GAO, *Missile Defense: Further Collaboration with the Intelligence Community Would Help MDA Keep Pace with Emerging Threats*, Washington, D.C., GAO-20-177, December 2019, p. 17.

[98] GAO, 2019.

[99] GAO, 2019.

Whereas products such as VOLT were frequently viewed as not adding significant value,[100] other required intelligence elements, such as CIPs, were viewed as useful. Improvements to the latter were also recommended, including expanding their use to all acquisition programs, not only ACAT 1D, along with providing earlier warning mechanisms when a CIP is breached. Intelligence professionals highlighted that CIPs were originally mandated only in DIA documents and guidance, but then became integrated into the JCIDS Manual and process, elevating it to be an integral element of the DAS process and as necessary intelligence support. This integration is an example of the utility of explicit policies, guidance, and processes, but it also illustrates how acquisition and requirement policy take precedence over that of intelligence in the DAS life cycle. PMs and requirements sponsors prioritize processes and documentation mandated in their guidance and policy documents, not those written by the IC. Therefore, while a variety of analytic products and inputs is provided by the IC, only those mentioned in acquisition or requirements policy regularly gain attention and have primacy.

Other interviewees noted that regulations requiring intelligence support in the form of specific product lines to acquisition programs lead to acquisition managers viewing intelligence inputs as a burden rather than a necessity (e.g., required product lines such as VOLT). Regulations appear to promote an agenda for the IC that tends to create products not entirely useful or timely, whereas intelligence support should be provided when it is necessary, more organic, and without explicit guidance. If intelligence agencies can demonstrate value to acquisition programs, then policy would not be necessary to force the relationship. While the interviewees generally agreed that the DAS

[100]Interviews characterized VOLT as a necessary document but not one that provided value on a daily basis. Many said VOLT was too thin on detail and lacked the engineering level of granularity to be useful to the program technically. A few program staff were not even aware of VOLT. However, the general consensus was that in spite of its problems, the VOLT was better than the STAR. That said, one interviewee indicated the replacement of the old System Threat Assessment Report (STAR) by VOLT was essentially the replacement of one useless document with another; he said he was directing his officers to disregard VOLT and produce products to the level of granularity he knows the programs want.

policies sufficiently direct programs to be threat-informed throughout the acquisition life cycle, because the DAS policies also emphasize cost, schedule, and performance, PMs are more willing to accept risk associated with threats that arise later in the program's life cycle in order to stay on schedule. On the other hand, existing the DAS policies serve to compel the program offices to engage with intelligence organizations.

Intelligence professionals interviewed expressed similar thoughts about intelligence policy and guidance on support to acquisition. Many cited the rescission of AFI 14-111 as an example. During IFTU training, instructors continued to refer to the document for direction on intelligence analysis for acquisition.[101] Most of our discussions with intelligence professionals, however, revealed less concern about the loss of the instruction itself, and more about what the instruction attempted to achieve. Multiple interviewees highlighted AFI 14-111's role as attempting to make acquisition integrate intelligence but noted that the instruction often fell short because it was not an acquisition policy document. "If it was an acquisition document that was rescinded, then that would be harder. The intelligence side marches on with production without it. . . . The acquisition documents make the program manager respond to us more than intelligence document," a former USAF intelligence professional told us. As previously discussed, our literature review covered both acquisition and intelligence policy documents. We observed that references to intelligence in acquisition documents was thin, focusing on when intelligence information and analysis are integrated into the DAS process, while the intelligence policy documents focus on internal intelligence processes. One intelligence professional went so far as to argue that even if AFI 14-111 was reestablished, institutional problems would remain due to a mismatch between the workforce and the knowledge required to support the DAS.

Our discussions also revealed concerns among some intelligence practitioners that DAS's Agile Acquisition Framework will become a

[101] Acquisition Intelligence Formal Training Unit, Wright-Patterson Air Force Base, December 2019.

potential challenge for the defense intelligence community. Some felt that internal DAF policies need to improve in order to address appropriate support to programs exercising rapid prototyping and rapid fielding authorities. Commensurate policy and guidance at the Air Force service level need to be tailored to the different acquisition pathways to ensure provided intelligence information will achieve desired effects. Others noted that rapid prototyping and fielding authorities will eventually fall into the same execution rhythm as the current MDAPs, if those authorities become the standard. But if the agile acquisition process can drive intelligence processes to be more agile, too, that would be a good thing. However, DAF needs to be cautious about adopting agile processes across all acquisition standards as some standards that might need agility the most (e.g., safety of flight and nuclear surety) are also the hardest to address.

Finally, some interviewees expressed that DoD-level policies also need to connect culture and policy, in a way that is similar to what DAF policies in other mission areas do. Making the decisionmaker responsible and accountable for meeting near-term intelligence requirements will create this connection. DoD-level policies also seem to have diluted language that directs the reader to see other regulations about integrating intelligence and acquisition, rather than readily providing the information themselves. This could also reflect DoD (and congressional) efforts to simplify policies and avoid replication.

Department of Defense and Department of Air Force Leadership Messaging

Published Material

Over the past five years, but increasingly throughout 2020, DoD and DAF senior leaders have emphasized the criticality of having threat informed acquisition processes. Echoing the themes of agility, experimentation, and risk-taking from the *National Defense Strategy*, CSAF General Charles Q. Brown, emphasizes in "Accelerate Change or Lose" the importance of internal collaboration within USAF. This collaboration is critical for the service to adapt to changes in the security envi-

ronment, by ensuring missions and capabilities are informed by and designed with U.S. adversaries in mind. General Brown further argues that cost, schedule, and performance metrics are not enough and that new metrics must explicitly measure adversary adaption and competitor timelines.[102] Likewise, while referring to the expanding capabilities of a near-peer adversary, the Deputy Assistant Secretary of Defense for China emphasized the importance of understanding adversary trend lines both to have a clearer picture of the intention of the adversary's current efforts and to be better able to predict future threats.[103]

This message is not limited to CSAF. In the AFMC Strategic Plan, released in July of 2020, General Arnold W. Bunch observed:

> Our adversaries have eroded our technological advantages and have presented us with new challenges and opportunities. These adversaries are rapidly innovating, improving, and developing future technologies with new warfighting expertise. We must operate at the speed of relevance to counter these threats and develop, deliver, support and sustain the most lethal and ready Air Force in the world.[104]

Furthermore, General Bunch included a call to action, asking for the development of "a recurring process to communicate command-wide comprehensive threats-to-acquisition to AFMC senior leaders and program offices to ensure the command is fully threat-informed" with a suspense five months after the publication of the plan.

Senior defense intelligence officials have likewise made statements specifically relating to improving intelligence support to the acquisition community. For example, on July 30, 2019, the Director of the Human Capital Management Office for the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]), released a memorandum supporting the awarding of a DoD-wide "foundational

---

[102] Brown, 2020.

[103] Tony Bertuca, "Pentagon Finds China Outpacing U.S. in Shipbuilding and Missile Tech," *Inside Defense*, September 1, 2020.

[104] Bunch, *AFMC Strategic Plan*, July 2020.

credential for Acquisition Intelligence within the Acquisition Intelligence Career Occupation Program."[105] This OUSD(I&S) memorandum recognizes the importance of establishing foundational training to prepare intelligence analysts to support the acquisition community.

These examples suggest that senior leaders are focused on ensuring that decisionmaking generally and that acquisition decisionmaking specifically are threat-informed. Continued public discussion and more explicit calls for intelligence and intelligence support to acquisition, however, remain critical, especially from acquisition senior leaders. Several of the statements implicitly do so by referring to intelligence functions (IMD, in particular) and the need to be threat-informed, but more explicit and frequent references might reinforce the criticality and necessity of the shift to threat-informed acquisitions.

Interviewees' Perspectives

In our interview, we asked about senior leadership messaging. At the working level, there was recognition of its importance. For example, RCO was forthright about this: "All PMs need to understand the nature of the threat, the NDS, and the risk of not acting quickly enough. There needs to be a galvanizing event, issue, or something else to force a change in mindset. It is a leadership imperative to inculcate a sense of urgency."[106] There was a mixed sense of how much leadership was stressing this in our discussions, many of which took place before CSAF's "Accelerate Change or Lose" and the AFMC strategic plan were published, so these were not reflected in the discussions.

Another way that leadership provides messages to staff is at command-wide briefings. These were described in multiple discussions in a positive way: Along with the information these briefings provide, they send the message that the leadership prioritizes this messaging. A recognized challenge is that threat information is different at different levels of clearance, which can be addressed by having different levels of briefings for different people. One commander who required receiving

[105] DoD, "Acquisition Intelligence Career Occupation Program Foundational Credential," Memorandum, Office of the Under Secretary of Defense, July 30, 2019.

[106] SME interview.

these briefings was referred to as "threat-savvy" by intelligence personnel. While this messaging was generally considered to be important and useful, some noted it needed to be backed up by necessary resources to ensure meaningful change.[107]

Findings and Recommendations

Finding: Acquisition intelligence is not considered an independent or unique field of intelligence support. Throughout DoD, DAF, and defense intelligence policy and guidance, the specific term "acquisition intelligence" is generally not recognized as a field of intelligence support with unique skills or knowledge. Instead, it is referred to as "intelligence support to acquisition," which is analogous to DIE support to policymakers and operators. AFI 14-111 specified "acquisition intelligence" as a unique field, providing specific definitions and expectations for intelligence analysts providing support to the DAS. As previously discussed, however, AFI 14-111 was rescinded and replaced by a more general Air Force manual regarding intelligence support in the department.

On September 11, 2020, the Office of the Under Secretary of Defense for Acquisition and Sustainment and OUSD(I&S) published DoDI 5000.86, *Acquisition Intelligence*. While it is placed under the structure of acquisition community guidance, it "establishes policy, assigns responsibilities, and provides direction for the integration of intelligence in the acquisition life cycle in accordance with DoDD 5000.01," delineating responsibilities for both the acquisition and intelligence community. The instruction calls for the creation of an acquisition intelligence career occupation program, which, over time, should increase the visibility of this unique field of intelligence expertise. This DoDI places the onus on both the acquisition and requirements communities for the inclusion of intelligence personnel and information in the entire acquisition life cycle. Most new policy, however, tells the

[107] We note here that recommendations might require additional resourcing, with the implication that there will be necessary trades between this and other needs.

acquisition system where and how to include intelligence information throughout the life cycle to "ensure agile and effective warfighting capability."[108]

Recommendation: If "acquisition intelligence" indeed requires unique product requirements and analyst skills, then DIE needs to understand that and prepare its analysts as necessary. Further implementation of the 2016 GAO recommendations would be a good start. OUSD(I&S)'s establishment of foundational credential for acquisition intelligence, incorporating Defense Acquisition University (DAU) courses, some of which are based on DAF's IFTU program, is a critical step. Moreover, updating DoD, DAF, and DIA policy and guidance as discussed in the next section might also improve intelligence support to the DAS, especially a DAS that is becoming more agile. The acquisition and intelligence communities must regularly discuss and assess the utility of intelligence products and processes to support the DAS and update them as necessary.

Finding: Acquisition is going agile; intelligence and requirements management should follow suit. As expected, our review of policy and guidance revealed that each community performs a different aspect of the DAS process: requirements focuses on identifying the requirements and capabilities needed, intelligence focuses on the providing insight into the threat, and acquisition focuses on delivering the capabilities as specified by the requirements community (schedule and performance) and as resourced by the financial management community and Congress (cost). With a push toward agile development, however, fixed requirements become less important, and ad hoc intelligence support to enable warfighters to determine more flexibly when a development satisfies their needs given threats becomes more critical. As a result, to support an agile acquisition process that is threat-informed, timelines to provide information become faster, with smaller, more tailored intelligence analyses and products required to match the more fluid, iterative requirements and development processes.

---

[108] DoDI 5000.86, 2020.

There is forthcoming updated intelligence policy and guidance from DIA that should define what intelligence support to acquisition is: maintenance of TL, VOLTs, CIPs, and management of multiple working groups between the acquisition and intelligence communities. This focus does not differ wholly from current intelligence policy documents. Moreover, these documents do not recognize or address the impact of the push for more agile acquisition programs. Thus, as the intelligence process currently stands, any ad hoc intelligence support to acquisition occurs through the routine production request process, wherein acquisition has to compete with other consumers (policymakers and warfighters) for intelligence time and attention.

Recommendation: DIE should continue to develop processes and methods to support and enable iterative and agile acquisition processes.

Finding: Policy and guidance, as well as senior leader messaging, do not consistently reinforce the importance of intelligence in the ecosystem. The policy and guidance of each community generally recognizes the ecosystem in which it participates, but the role that intelligence plays should be further clarified. Both requirements and acquisition address the importance of intelligence for their operations as a supporting element, but there are instances when reinforcing the importance of intelligence can help strengthen this recognition within each community in the ecosystem. Challenges include acquisition guidance focusing on cost, schedule, and performance targets and intelligence having acquisition as a third priority after near-term tactical and operational intelligence support to the warfighter and strategic intelligence support to the policymaker.

Recommendation: Future policy and guidance updates and senior leader messaging should, where appropriate, stress the importance of meeting the current and envisioned future threat along with the nexus of intelligence, requirements, and acquisition and especially the symbiotic relationship between intelligence and both requirements and acquisition to achieve threat-informed

acquisition.[109] Additional recommendations for further consideration include consistent senior level messaging on the changing nature of the threat and the necessity for threat-informed decisionmaking, including in support of requirements and acquisition and regular threat briefings at appropriate organizational levels, which should help ensure staff maintain focus on the threat as it relates to their work.

While senior leader messaging is important to the enterprise, it is insufficient to generate change. Translating vision into action requires resources, and prioritizing threat-informed acquisition will require additional investments in funding so that acquisition programs can adapt to the threat, acquisition personnel can understand the threat, intelligence prioritizes supporting acquisition, and so forth. Since resources are not unlimited, this needs to be a prioritized decision—tempered, of course with trade-offs given the importance of other demands on resources. Hence we recommend that if threat-informed acquisition is truly a priority, resources should be made available to support it. This might mean taking resources away from lower-priority needs and processes.

---

[109] DoDD 5000.01, 2020, again focuses on the DAS life cycle, and not the critical role of intelligence for threat informed or agile acquisition. "Threat" is mentioned only once, and in a subsection related to testing and evaluation. OUSD(I&S) responsibilities focus on IMD, CI, and security concerns, with no mention of threat assessments or integration of threat information into the DAS life cycle.

CHAPTER FOUR

Improving Information Flow Between Intelligence and Acquisition

In this chapter, we discuss information sharing between the acquisition and intelligence communities. Such information sharing can be characterized in terms of demand and supply. The acquisition community needs finished, validated intelligence to ensure systems and equipment developed keep apace of adversary threats, whereas the IC's task is to ensure that those questions are addressed. The requirements community also receives significant intelligence support, but they receive it differently. The requirements community uses finished intelligence as well as information from professional and academic sources and national laboratories. Unlike the acquisition community, which is generally required to use "validated" intelligence, the requirements community has no such requirement. There is an intelligence "trail" that is passed from the requirements to the acquisition community, and that is reflected in drafting the first VOLT.

In USAF's acquisition-intelligence environment, demand for information can be either formal or informal. Some products that the IC provides to acquisition emerge from formal demand processes and procedures. Others derive from ad hoc interactions and constitute informal demand exchanges. This chapter discusses how these two demand strands are integrated and offers recommendations for strengthening the information flow. This is a challenge, given that the acquisition community's "demand signal" for intelligence has often been incompletely communicated to and understood by the IC, which has diminished the IC's ability to provide acquisition programs with

the scope and detail of data required. The goal of this chapter is to improve USAF leaders' understanding of information sharing's integration challenges and to identify mitigating strategies regarding the identification of requirements and flow of data.

The chapter begins with a look at the current processes used to identify, produce, and share information between acquisition and intelligence and identifies strengths and weaknesses. It then combines information distilled from discussions the project team held with SMEs on best practices in information management and their recommendations for improving communications between these two communities so that acquisition decisionmakers have the critical threat information they need.[1]

Overview of Intelligence Production and Sharing Processes

Intelligence Production Processes

The IC collects and produces finished intelligence in support of the intelligence requirements of the defense acquisition community. The finished products are available on the Joint Worldwide Intelligence Communication System (JWICS), Secure Internet Protocol Router Network (SIPRNet), and other systems and at various classification levels, so they are accessible and discoverable by individuals and organizations needing intelligence support. All the intelligence disciplines—human intelligence, signals intelligence, GEOINT, measurement and signatures intelligence—collect and report information based on collection tasks. This information is used by all-source intelligence analysts, principally at the Central Intelligence Agency, DIA, NSA, and

[1] From 2013 to 2017, RAND supported an effort by AT&L's Performance Analysis and Root Cause Assessment office to assess the effectiveness of the IC's delivery of threat intelligence to acquisition programs. That research showed that the demand signal for intelligence from programs could not be evaluated because there was no single location for registering and managing those tasks, and there was no regulatory requirement to do so. RAND research supported the development of a digital tool to facilitate this process. Work on the tool was set aside in the recent elimination of USD(AT&L) and establishment of USD(A&S).

the service intelligence production centers (e.g., NASIC), to produce products responding to the needs of national security and defense consumers, including acquisition programs.

The vast numbers and broad needs of consumers of intelligence result in competition for intelligence collection, production, and dissemination among consumers. Deployed U.S. military forces led by the combatant commands (CCMDs) in areas of hostilities always receive immediate attention. CCMDs have large, organic, direct-support intelligence staffs, and deploying forces generally have attached intelligence units that depend on "reach back" to intelligence staffs located in the rear whose task is to satisfy deployed force requirements. Similarly, national-level policymakers almost always receive immediate attention. Policy and intelligence have long enjoyed a close relationship, and many policymakers occupy visible positions that demand high-priority responses. Lacking the immediacy of warfighters or the prominence of policymakers, acquisition community members must compete for attention to get intelligence support.

To compensate for finite resources and to try to satisfy production requests to the extent possible, the IC gathers information requests from consumers on a recurring basis, annually (through the NIPF) if not more frequently otherwise, and develops a program of production that seeks to address those requests. DIA manages DIAP, which integrates general military intelligence and S&TI production conducted by DIE, including DIA, CCMDs, and the service intelligence centers. DIAP seeks to focus all-source defense intelligence analysis efforts on the highest priority issues for defense customers, while limiting duplication of effort.

Production of intelligence is generally governed by a program of analysis (PoA) at each intelligence production center. PoAs aim to address as many consumer questions as possible. Each production organization has a specific requirement to produce intelligence for its key consumers, but no single intelligence organization has the expertise or resources to address all questions. To ensure that the IC develops products that address the full range of information needs of consumers, DIAP seeks to ensure that all questions are addressed by the organization with the greatest direct expertise on the issue. DIAP identifies

more than 200 intelligence production requirements, including at least two specific intelligence requirements concerning support to acquisition programs.

Intelligence organizations have PoAs that identify their priorities and the products to address them. The NASIC PoA includes its DIAP tasks as well as production requirements specific to Air Force consumers. It seeks to satisfy the broad range of intelligence customers in its production plan. Acknowledging that it cannot produce all the products its consumers, and principally Air Force, need, NASIC prioritizes its production resources according to three levels:

- primary resources put to known current threat
- secondary resources put to known future threat (next)
- tertiary resources put to unknown future threat (after next).

The implication of this ordering is that supporting traditional acquisition programs may come after supporting the warfighter (along with perhaps some rapid acquisition programs).

Interviews with intelligence and program staff describe a task system that depicts a two-step transactional approach. In the first step, acquisition intelligence officers identify needs. In the second, the officers seek to fulfill those needs either by finding answers in the intelligence database, consulting with analysts at the Intelligence Production Centers (IPCs) to determine whether there are existing answers that can be provided, or tasking a production requirement if no answers exist. Interviewees reported that downward negotiation of a production requirement, a situation in which the producer identifies what can be provided as opposed to what the consumer actually needs, occurs regularly. Having a requirement rewritten to seek only that which is available denies the IC the resources to identify intelligence production and collection gaps that need attention. If gaps are not identified, the IC has no way to discover them and take appropriate action to close them. Additionally, downward negotiation might not mean that the IC does not have the information or the expertise. It might simply mean that the producers did not have time to address all the questions so identified or that the task was not well understood by the intelligence

analyst. Recall, however, that the acquisition community may have the demand for more intelligence than the IC can provide (more quantity and specificity), so downward negotiation may sometimes be necessary.

One area of special concern for many program and intelligence officers is the absence of long-range intelligence forecasting and futures intelligence. Many programs—especially those in the early, pre–Milestone A phase—need forecasts of possible developments out 25–30 years, which is the likely lifespan of their capability. While they acknowledge that VOLT provides some future-oriented intelligence, they believe the brevity of the analysis is insufficient for their needs. Several interviewees expressed their view that a U.S. technological edge was no longer a valid assumption and that intelligence collection and analysis failed to consider knowledge of adversaries' future research and development competencies that they could militarized in the near term to generate unexpected threats to U.S. systems, capabilities, and interests. Academic and professional discussions on potentially disruptive technologies that might tilt the balance of power away from the United States exist, but are not sufficiently developed for use by requirements and acquisition officers who need to be able to cite U.S. intelligence analysis as a basis for decisions as their programs move forward.

Intelligence Products and Databases for Acquisition

For the acquisition community, DIE produces a variety of specialized products including military capabilities studies and technical assessments of adversary weapon systems, platforms, and equipment, and military facilities, among others. Some products result from planned and scheduled production; they contain significant characterization and analytic detail. Intelligence producers also publish shorter, more current analyses that aim to alert consumers to information that updates or changes existing published studies and threat assessments. The shorter, current intelligence documents aim to inform consumers of evolutionary threats that need to be considered in their decisionmaking.[2]

[2] There is a difference between planned intelligence production and initiative ad hoc production, or current intelligence, which seeks to update existing analytic conclusions by updating the information and identifying any nuance of change to the standing product.

A final category of products includes ad hoc responses to individual questions raised by individual consumers, including program offices. Interviews suggest that program offices consider this intelligence support to be especially significant because it provides detailed information at an appropriate technical level that to the extent possible ensures the equipment being developed continues to be able to meet an evolving threat. Interviews with acquisition intelligence support officers suggest that these ad hoc queries are their most frequent task. Tasking, tracking, and leveraging these ad hoc tasks are discussed below.

Two notable intelligence products are unique to the acquisition community: the VOLT assessment and the CIP documents.

- VOLT is specified in DoDI 5000.85, *Major Capability Acquisition*. That document does not expressly use the term "VOLT," but it imposes information requirements that are spelled out in the Non-classified Internet Protocol (IP) Router Network (NIPRNet) website Milestone Document Identification (MDID) and treats those requirements as if they are written into the instruction.[3] DoDI 5000.86, *Acquisition Intelligence*, also mentions VOLT, identifying VOLT as a document supporting programs, though not mandating its use.
- VOLT is the authoritative threat assessment tailored for each specific program. It supports capability development and PM assessments of mission needs and capability gaps against likely threat capabilities at initial operational capability. According to the latest guidance available, VOLTs are prepared prior to entry to Milestone A and again for entry into Milestone C. An update to a VOLT report might also be sought for nonmilestone issues.

These short-term products are the ones that acquisition intelligence officers generally deliver to their programs as the production arrives. An issue might be that small, evolutionary changes that are important to intelligence analysis might not be as valuable to consumers until those changes build up into something greater or something that surprises consumers.

[3] See DAU, undated(b).

- CIPs represent key performance thresholds of foreign threat systems, which, if exceeded could compromise the mission effectiveness of a fielded or developing system. The CIP requirement is driven by the JCIDS process; CIPs are required for threat-sensitive programs. CIPs are developed collaboratively between intelligence and program stakeholders. They are supposed to be established early in a program's life cycle so that the IC can monitor capability advances by key adversaries and report breaches throughout the life cycle of a program, but especially prior to major program decision points.

In addition to these specialized and ad hoc products, DIA, the other national intelligence agencies, and the service intelligence centers populate and maintain databases that are available at several levels of classification and are designed to allow nonintelligence professionals to "pull" needed information. Several products and databases specifically serve the acquisition community. The largest and most frequently used databases include the following:

- TL, maintained by DIA, houses around 300 modules of finished, validated, and current intelligence on threats to U.S. weapon systems. Data stored in the TL fall into one of seven general categories: weapons; sensors; platform/targets; countermeasures; chemical/biological/radiological/nuclear; strategy/doctrine/employment; and cyberspace. TL is available on JWICS and SIPRnet. TL is composed of the threat modules that represent DIE's official assessment of the principal threat systems and capabilities that a potential adversary might reasonably bring to bear in an attempt to defeat or degrade U.S. systems and capabilities. TL is a primary source of intelligence threat information for preparation of VOLT, discussed below.
- The Military Equipment and Parametrics Engineering Database houses scientific and technical characteristics and assessments of foreign weapon systems. Information in the database is generally used to assess equipment capabilities and identify equipment based on its electronic emissions. This database provides infor-

mation critical to operators who need IMD to support ongoing operations.
- The Modernized Integrated Data Base provides characterization of foreign military forces and facilities used to assess military capabilities. It is being replaced by the Machine-Assisted Analytic Rapid-Repository System, which aims to use artificial intelligence and machine learning capabilities to enable simulation of adversary courses of action, which should be an improvement over the static databases currently in use.

Production Requirement Tasking and Tracking

In addition to substantive databases, the IC provides a cross-community tasking system that serves as a vehicle by which intelligence consumers can task intelligence producers for support. Community On-Line Intelligence System for End Users and Managers (COLISEUM) is a task registration and management tool for defense intelligence. Originally designed in the 1980s to facilitate intelligence support to the acquisition process, it evolved into a system to handle all defense requirements and, more recently, to support DIAP. At present, COLISEUM is considered a one-stop shop for organizations to task one another on all standing defense requirements and on ad hoc taskings from customers. COLISEUM is designed to be used as a cross-organization task-registration and management system; it does not replace internal tasking mechanisms within the services.

COLISEUM has several functions that are ancillary to its status as a task-registration system. VOLT requirements are generally registered in COLISEUM. Use of COLISEUM to register the VOLT requirement alerts production elements across the community of the requirement. This registration location also can be used to inform acquisition and intelligence organizations. Additionally, COLISEUM serves as the single repository for CIPs, which outline key performance thresholds of foreign threat systems that, if exceeded, could compromise the mission effectiveness of a U.S. weapon system.

Most intelligence officers supporting acquisitions found COLISEUM to be slow and awkward. While it is possible to submit a requirement into COLISEUM without pre-coordination, almost all who

worked with COLISEUM noted that it benefits from pre-coordination through an informal network to ensure the task is aligned with production capability. Pre-coordination is used to prevent requirements from being refused in the system. Most acquisition intelligence support officers coordinate with an analyst at NASIC either just before or after submitting a production request. Often, a pre-coordination call results in a quick answer, but that information is often not captured in COLISEUM or made available to a wider audience, and no one gets credit for the action. Users also said COLISEUM is opaque in reporting the status of a production request. Once a request is submitted, especially if there is no pre-coordination, it is difficult to ascertain where a request is in the process or when to expect an answer.

Another shortfall of COLISEUM in supporting the acquisition community is that it does not service special access programs (SAPs). Interviewees reported that COLISEUM's classification limitations prevent it from being used to handle SAP material (although very limited alternative systems may exist). This drives them to use their informal network of contacts across the IC. One interviewee said, "That's the biggest thing I hear from program offices, 'If you were not here, we would not have known that.'"[4] This interviewee cultivated relationships with organizations that volunteer information that the program needs to better meet intelligence requirements.

As a knowledge-management system, COLISEUM was characterized as extremely outdated. Search algorithms returned unrelated results, there are no simple ways to search past answers to similar questions, and the ability to search for all intelligence for one system and compare it with a next-generation system is not possible. Despite these shortcomings, many still found COLISEUM at least somewhat useful and good enough when coupled with other available intelligence support avenues.

Intelligence Dissemination and Sharing Processes

While program offices' need for a continuous flow of intelligence is well established, the doctrinal requirement for intelligence products in the acquisition process is much more restricted. DoD guidance on

[4] SME interview.

formal intelligence support for the "processes" focuses on documentation prepared for milestone reviews. For example, VOLT is prepared for programs entering Milestone A. Other acquisition documents, such as ICDs and CDDs, require intelligence inputs, but not separate documentation.

Flagship intelligence products such as VOLT and technical databases built and maintained for the acquisition community, such as TL, represent only a part of the flow of information to acquisition programs. Regular, even daily, contacts between program offices and intelligence personnel generate many ad hoc requests for intelligence. These requests are initially received by acquisition intelligence officers supporting individual program offices. These intelligence officers take responsibility for providing a response. In some cases, answers can be found in existing databases. If no answers are available, a production request is developed and sent to the appropriate production center for action either through an internal tasking system or through COLISEUM. Intelligence production requests result in official intelligence products that are returned directly to the requester. Intelligence support personnel who reside in program offices or who have liaison responsibilities regularly deliver information, either on their own initiative or in response to informal questions.

The formal and informal methods for identifying intelligence questions and producing responses to those questions are transactional and may not entirely capture programs' intelligence needs. PEOs and program offices do not have established lists of priority intelligence requirements (PIRs), which serve to guide and prioritize intelligence production over time. [5] Intelligence products responding to program requests can generally be characterized as ad hoc support, as there is no discernible "theme" to any program's intelligence requests. Interviews with acquisition and intelligence professionals confirmed that there is no single, overarching process for determining and codifying

[5] PIRs are common service and command documents, which are used to identify key priorities and to guide intelligence collection and production. Similarly, the national policy community has the National Intelligence Priorities Framework and maintains the Integrated Defense Intelligence Priorities, which reflects the priorities of DoD missions and functions that rely on DoD intelligence support.

a program's threat intelligence needs, levying production requirements for meeting those needs, and then sharing threat information with the program and potentially with others interested in the analysis.

While interviewees emphasized challenges with the formal process, many mentioned informal mechanisms through which the communities communicate. A formal mechanism is TWG, a forum used by program and intelligence officers to share information, discuss program needs, and codify specific threat intelligence tasks. TWGs appear to exist at several levels; some individual programs have TWGs, while other TWGs appear to exist at a higher level, including at PEO. While TWGs were not frequently mentioned by interviewees unless prompted, they were described as both a forum for identifying and codifying intelligence requirements, but also as opportunities that promoted relationships and trust-building between program offices and intelligence support staffs.[6] There is no single repository that captures all threat intelligence tasks for all programs, and there is no good place, including COLISEUM, that can be exploited and studied to assess the overall "demand signal" for threat intelligence.

---

[6] There is no specific reference to TWGs in guidance documents, but they are generally comprised of the same stakeholders as TSGs, which are defined in guidance. DIA guidance issued to implement threat intelligence support requirements highlighted in DoD 5000 call for the scheduling of a TSG for ACAT 1D programs. DIA co-chairs the meeting with the military service component or the intelligence production center having responsibility for threat support to the program and for VOLT review and validation. TSG membership includes the capability developer/requirements sponsor, the PM or representative, the military service test representative, and the Director of Operational Test and Evaluation representative.

Our discussions identified one instance in which a program office developed a local memorandum of understanding (MOU) with its intelligence support officers, which seeks to routinize the early identification of threat requirements, which are in turn tasked to intelligence producers. In this case, producers have longer production timelines and the program has greater control over the scope and arrival time of intelligence support to the program. Additionally, MOU provides the skeleton of a framework for creating a history of intelligence support to the program, which facilitates rotation in and out of positions by individuals in both communities. MOU appears to have the ability to present, over time, a demand signal for the program it supports; program and intelligence personnel could review the document and products tasked and delivered, develop follow-on requirements as necessary, and at least informally better understand the impact that provision of timely threat intelligence has had on the program.

In addition to TWGs, a substantial amount of information flows between the acquisition and intelligence communities through informal channels grounded in personal relationships, often referred to colloquially as the "bro-net" or "sneaker net." One interviewee from an intelligence squadron commented, "The customers usually reach out to us via the relationships we've built with them over the years (what the military typically calls the 'bro-net')."[7] While informal networks typically lack official guidance or record-keeping policies associated with their use, they are critical to maintaining information linkages between sometimes disparate elements of the acquisition-intelligence system. We refer to them as informal networks because they arise organically from personal relationships that build up over years.

We spoke with dozens of acquisition and intelligence personnel who cited the importance of these informal networks in disseminating critical threat information. A common and persistent thread in these discussions concerned the speed and ease with which acquisition personnel could obtain information by, for example, calling a colleague at NASIC instead of putting a production request into COLISEUM. An intelligence officer told us, "Sometimes, the level of bureaucratic investment is not worth the information provider and requester's time when something can be simply answered."[8] When production requests were necessary, several interviewees indicated that they relied on informal pre-coordination of the request via existing relationships with intelligence analysts to ensure a timely and accurate supply of information. Furthermore, many interviewees indicated that intelligence contacts whom they knew from previous roles or personal friendships were the essential—and in some cases, the only—touchpoint they had with anyone in the IC. See Table 4.1 for representative views.

While a range of push-and-pull mechanisms for information exchange exists at varying levels of formality—from TSGs and TWGs to various other arrangements at or inside of specific PEOs—effective information management, both within and across the acquisition and intelligence communities, currently depends heavily on what one inter-

[7] SME interview.

[8] SME interview.

Table 4.1
Illustrative Quotations from Acquisition and Intelligence Personnel

Importance of informal networks	"The customers usually reach out to us via the relationships we've built with them over the years (what the military typically calls the 'bro'-net). We get so many varied requests and do most of our time providing interchange/liaison between organizations that when we've tried to make a system to interface with us, it's either ignored or not relevant because the requests are so varied. Almost all folks reaching out to us either come in through a person they know, or potentially through some org-mailboxes we've set up (though those are infrequently used as well). To be frank: it's strange to me how 'sticky' external agencies become with individual analysts or teams. It shows how much value is placed on people/teams doing unique missions over a specific process, because even when we set them up, external orgs/agencies gradually and sometimes rapidly drift back to one-on-one relationships."
Need for pre-coordination	"We use COLISEUM effectively when we have a preexisting relationship and conversation. We pre-coordinate the work and then use COLISUEM after. If you don't, you get garbage back. It looks like NASIC accepts the req and nothing happens until it's due. Then you get requests to extend the suspense, nothing happens. The "bro-net" is the only thing that works. NASIC doesn't understand our programs or needs. We have to explain it to them."
Shortcomings of informal communication	"Need to capture informal communication—old school ways no longer work; professional moves will break networks; knowledge management and relationships with IPCs are currently awful."

SOURCE: RAND interviews with Air Force acquisition and intelligence personnel.

viewee called "tribal knowledge." Essentially, individual personnel may know whom in the ecosystem to contact informally, but there is little to no systematic documentation of these relationships or the information that gets shared through them. In other words, when knowledgeable individuals move on from given positions in the acquisition or intelligence community, they typically take the relevant information and connections with them.

Information-Sharing Impediments

During our discussions with SMEs from the acquisitions, requirements, and intelligence communities, we elicited significant data on information-sharing impediments. These interviews provided signifi-

cant context and painted a detailed picture of the physical and technical impediments of information sharing among those communities.

Lack of Cleared Staff

One clear theme of the interviews was that there are too few people with the right clearances in the right positions. Intelligence personnel working in acquisitions often face challenges with not having enough program counterparts with the right clearances and cumbersome clearance processes. Many program offices said that more people at their organization had only secret clearances when the threat was reported at the top secret (TS) level. An interviewee commented, "Part of the limitation [of intel] is that it's on JWICS. TS/SCI [sensitive compartmented information] system access is not widespread in the portfolio."[9] While leadership might have that clearance, tactical and engineering decisions were hampered by personnel without access to information. Some groups reported that all PEOs are cleared at the appropriate SCI level but that most PMs' clearances are below SCI and therefore too low to weigh in on decisions. Only one group reported having the right billets for cleared personnel, but that those billets were not being filled at the time.

Several interviewees believed the problem with the lack of security clearances is that most program staff positions are not required to have security clearances prior to being hired. Some officers may be cleared over time, but these clearances are tied to the individual, not the position. This situation can be difficult for offices where individuals move to new positions, taking their clearances with them and leaving behind uncleared successors. One interviewee observed that clearance levels often seemed disregarded, inasmuch as engineers and other key staff with appropriate clearances were rotated out or reassigned to other projects with little regard for matching the replacing officer with the clearance to the billet. The effect of having too few people cleared at the right levels is that there are not enough people to receive, analyze, and incorporate collected data into their work.

[9] SME interview.

Problem-solving discussions are also limited, as not all contributors could discuss aspects of the threat and the program together.

Programs also have a hard time hiring and retaining cleared people. Program offices compete with contractors who can hire good scientists without clearance, pay them well, and obtain a clearance for them six months later, while most programs cannot hire until personnel have a clearance. The backlog in the system hurts recruiting and retention of qualified intelligence and program personnel and the actual work of the acquisitions programs.

Difficulty in Accessing and Using Special Access Program Material

Access to SAP information is a major obstacle for collaboration between intelligence and acquisition. Intelligence staffs also reported little or no access to SAP information controlled by the program office and difficulty using SAP information to which they had access. Often, IC analysts are not read into acquisition program SAPs; therefore, they cannot adequately assess how adversary capabilities can affect friendly programs, because they are not experts in friendly capabilities.

The nature of SAP is to limit access to program information except to those who need to know. Some programs refuse to work outside of SAP channels. This essentially stovepipes information and excludes most intelligence personnel, who are not considered need-to-know colleagues. Absent intelligence analysts having access to SAP information, some acquisition personnel were left to write their own threat reports, integrating intelligence and SAP information before sending it back to an intelligence analyst for peer review. Having intelligence staff with the proper clearances and with access to SAP information is essential to reducing stovepiping and ensuring intelligence personnel are informed and are writing threat-informed intelligence products.

If gaining access to SAP material is difficult, using it in intelligence products is also a problem. Sharing the analysis is limited so that only those with both intelligence and program clearances can have access. SAP creates degrees of segmentation that make it difficult for acquisitions personnel to explain to colleagues in the IC why they need certain things at certain times and to explain to leadership why certain things are available or unavailable at other times. Because of SAP,

those in the same directorate working on similar programs or issues are sometimes unable to share information or help each other. A few groups are trying to eliminate those barriers across similar programs by putting all programs under the same level of SAP access, thereby giving all personnel with SAP access visibility to all programs in the portfolio. This is followed up with conferences to update all SAP access personnel on the progress of each program. While including intelligence analysts in these conferences may help bring intelligence threat information to programs, one or two of our interviewees voiced concerns about malicious or negligent insider threats. The risks of allowing access to SAP would need to be weighed along with the benefits of including intelligence in SAP discussions.

Not Enough Access to Classified Computing

Many intelligence officers supporting acquisition programs work in the program offices or visit them regularly. Analysts, however, need adequate secure or sensitive compartmented information facility (SCIF) space in or near these offices to access intelligence materials and to collaborate with fellow analysts so they can do their jobs effectively. The lack of JWICS access was a constant theme in interviews. Some interviewees also said that secure facility space constraints mean that SIPRnet is not always an available alternative. Interviewees reported a spectrum of SCIF availability in program offices. Some have no SCIF access on-site or nearby. Some have SCIF access, but the space is too small to collaborate with others. One interviewee commented, "Even if we had the JWICS terminal, we would have to hide it in a closet. There are no rooms in the office to have a TS/SCI conversation, store documentation, etcetera."[10] Some share SCIF space with other people, making it hard to schedule time on a terminal. Some had very inconvenient access to a SCIF and thus did not use it often. Still others had to borrow space from other programs in ways they perceived to strain the relationship with the owners of the SCIF. Only a few programs, dealing mostly with cyber, reported they either had enough SCIF space or that it was being built or leased.

[10] SME interview.

The lack of classified communications capability means that program staff might not have access to JWICS and SIPRnet where they would be able to find and extract pertinent information from the TL and technical databases. Intelligence officers may be reduced to hand-carrying intelligence products to their customers. Hard-copy materials limit availability to others in the program office. Additionally, hard-copy items are not always discoverable in classified databases, assuming the documents are stored electronically and made available for discovery.

As with SCIF spaces, there is a shortage of facilities approved to handle and store SAP materials. An interviewee stated, "[Our organization] does not have a SCIF. . . . We're trying to build a secure room so we can deal with some of the classified and SAP aspects of our programs. . . . This has been a huge limiting factor. . . . I have to walk halfway down a building and schedule time. We have a 300-person organization and share with [an] office of 160 people and we have one SIPR terminal."[11] Several groups reported combining or wanting to combine their SCIF with a SAP facility so that analysts and engineers could work fluidly on threats. They said they needed these dual spaces accredited for both SAP and SCI to integrate and address threats at the classification for which they are cleared.

Interviewees who have regular access to JWICS and SIPRnet have markedly different views than those who did not. Important databases, including TL, are accessible on both SIPRnet and JWICS. Nonetheless, most prefer to keep information at the NIPR level to avoid the inconvenience of working with data on SIPRnet or JWICS. Reaching someone at NASIC usually means reaching out over JWICS, which, in turn, limits direct interaction between many program office staff and intelligence producers.

TL is generally viewed more favorably by interviewees. It is seen as sufficient for less-specific threats, for providing information for VOLT, and for sometimes being customized to particular programs. It falls short in interviewees' eyes when they need more granular intelligence

[11] SME interview.

to support a program or when acquisition leaders see TL as a way to check a box before moving forward.

Integrating Academic Research with Existing Processes

Academic research and professional studies examining how information is shared between and among groups of individuals and expert communities underscore a common theme: Interaction between formal structures and informal coordination practices is critical for generating and sharing knowledge through delegation of responsibility, deconstruction of problems, and awareness of dependencies.

Interaction Between Formal and Informal Structures

For team-based projects, formal structures are important for mapping out how personnel with various functional specialties might be paired up (such as embedding an intelligence analyst with a program office). But equally important are informal coordination interactions that influence how work *within and across* those teams is accomplished (by connecting that program to the wider IC).

Within teams, successful informal coordination results when specialists (1) informally anticipate how others' work might affect their own or compromise their own domain-specific standards of excellence, (2) synchronize workflows to match time interdependencies, and (3) triangulate domain-specific findings against other benchmarks.

Across teams, informal coordination succeeds when specialists from other domains force others to "externalize their tacit knowledge" by questioning underlying assumptions. Organizations can support these interactions by implementing programs to mentor and train specialists, convening project debriefings, and holding periodic social events.[12] Further, when formal structures do not have the intended results, informal networks might be critical to bridging those gaps.

---

[12] Shiko M. Ben-Menahem, Georg Von Krogh, Zeynep Erden, and Andreas Schneider, "Coordinating Knowledge Creation in Multidisciplinary Teams: Evidence from Early-Stage Drug Discovery," *Academy of Management Journal*, Vol. 59, 2016, pp. 1319–1320, 1333.

Within informal networks, organizations also must be attentive to the various types of individuals who participate in the interactions beyond whether they primarily provide or acquire information. For example, innovation often occurs when "information brokers" fill "structural holes"[13]—or put differently, when people or groups start to fill in gaps in information flows between subgroups within larger organizations. By helping identify how the needs of one group might be addressed by the skills in another, these brokers can be pivot points for new combinations of information.

Lessons from Academic and Professional Literature

The lessons from the research team's academic and professional literature review comported closely to the findings of the research conducted with intelligence and acquisition practitioners. Formal and informal information flows within organizations exist but informal communication networks are both ubiquitous and vital. Indeed, successful collaboration, especially in research and development–intensive fields, often hinges on effective and efficient information sharing. Our research found that the acquisition and intelligence communities use many means of communication but that these are often hindered by absence of a common vocabulary and a system that can accommodate the sensitive information shared between the two communities; factors such as the nature of the information itself and the channels used to communicate that information can make the exchange of knowledge challenging. Informal communication can be both a critical enabler and an impediment to information transfer.

Tacit Versus Explicit Knowledge

Our first lesson is that the nature of knowledge itself might hinder the effective exchange of information.[14] Especially as knowledge of technology has become more specialized within disciplinary boundaries,

---

[13] Ronald S. Burt, *Structural Holes: The Social Structure of Competition, Harvard University Press*, Cambridge, 1992.

[14] Here, we consider "information" as raw data and "knowledge" as the ability to apply that data toward the achievement of some goal. We do, however, use the terms interchangeably at various points below.

and is thus shared imperfectly over time and among people, organizations, and industries, the importance of collaboration across these divides in matching problems with solutions has only grown.[15] Issues with sharing knowledge arise, however, because there are at least two different types—tacit and explicit.

Tacit knowledge captures the notion that individuals often seem to know more than they can explain; it has a personal quality that is hard to formalize or communicate and is frequently rooted in individual experiences or involvement in a specific context. By its very nature, tacit knowledge is difficult to process, share, or store in a logical or systematic way.

In contrast, *explicit knowledge* takes the form of factual data or fixed content that can be articulated and shared through formal, systematic language as well as being easily processed or stored.[16] For example, natural sciences such as chemistry and biology are built on empirical regularities that researchers use to develop and test hypotheses through observation. In principle, this process generates explicit knowledge through the value-free and objective nature of observation. In practice, however, both technical and cognitive elements of tacit knowledge have enormous influence over the conduct and success of scientific research, whether in terms of the hard skills needed to carry out experiments or the soft skills required to generate original research questions, recognize patterns, and make intuitive judgments.[17]

While tacit knowledge can be a key enabler of scientific progress, it might not easily transfer among individuals who do not share backgrounds, skill sets, or experiences, which is often the case between intelligence officers and the acquisition community, in which individuals are more likely to have technical backgrounds. We observed many examples of tacit or "tribal" knowledge through our interviews. Mem-

---

[15] Andrew Hargadon and Robert I. Sutton, "Technology Brokering and Innovation in a Product Development Firm," *Administrative Science Quarterly*, Vol. 42, No. 4, 1997, p. 716; Benjamin Niedergassel, *Knowledge Sharing in Research Collaborations*, Springer Science and Business Media, 2011.

[16] Niedergassel, 2011, pp. 3–4.

[17] Niedergassel, 2011, p. 222.

bers of the acquisition and intelligence communities might not recognize it as such, but much of what they have come to know through personal relationships (i.e., whom to call in a particular situation) and domain-specific expertise (i.e., about a particular program or system) qualifies as tacit knowledge to the extent that it might be hard to formalize or is rooted in specific experiences. This is not unusual or normatively negative; however, it poses challenges for systematizing information exchanges in ways that do not rely as heavily on knowledge or expertise held only by certain key personnel.

Asymmetries in Information Sharing

A second and related lesson from the literature review is that various parties within and across organizations might act as acquirers or providers of information, with varying incentives to share data depending upon which role they are filling. Situations of asymmetric interdependence can arise from an uneven distribution of knowledge—in other words, an employee might need data from a colleague to complete a task, but the latter might not be similarly reliant on the former. Transferred knowledge might be beneficial for the acquirer, but costly for the provider, as the process often involves specific investments of time and energy that might or might not align with the latter's time restraints or professional incentives. Though information providers might not overtly refuse to help colleagues, there is reason to expect significant variation in the effort they devote to those requests and the quality of the ultimate output.[18]

This issue can cut in both directions where acquisition and intelligence are concerned. Most important, from the intelligence perspective, fulfilling the acquisition community's production requests may be costly relative to other priorities, such as supporting the warfighter or the policymaker. Even if programs would benefit from better intelligence, analysts are often not incentivized to invest the time and energy in the face of more pressing professional imperatives or more pressing deadlines. Meanwhile, from the acquisition perspective, receiving or

[18] Martin Gargiulo, Gokhan Ertug, and Charles Galunic, "The Two Faces of Control: Network Closure and Individual Performance among Knowledge Workers," *Administrative Science Quarterly*, Vol. 54, 2009, pp. 302–304.

requesting intelligence is not always viewed as strictly necessary for acquisition personnel to perform their jobs. It can be costly to programs to ask for intelligence on a particular threat if the information is not going to arrive quickly or leads to slippage in cost or schedule. This means that intelligence simultaneously lacks both incentives to support acquisition and a demand signal for its services, given that acquisition is not (or does not always view itself as) strictly reliant on intelligence to perform its duties.

Group Cohesion and Quality of Collaboration

Academic research shows that networks with higher levels of social cohesion and connectedness across knowledge pools improve information transfer.[19] Having similar training and stronger interpersonal connections makes it easier to share knowledge. This has implications for information flows from the IC to acquisition, which does feature informal knowledge transfer, as we have discussed. These incentives and opportunities exist to some extent for acquisition and intelligence through forums such as TWGs, but more frequent chances for these communities to convene and make connections could contribute to greater cohesion and range in their personal relationships. Additionally, the establishment of DoIs around the Air Force acquisition community is another opportunity to cultivate relationships that will improve the climate for information exchange between the communities. In interviews with SMEs, we consistently heard from program offices that assigning DoIs directly to the program staff (instead of to an offsite intelligence office) means that stronger relationships will be developed and that non-intel program elements will have greater "trust" in their intelligence counterparts.

Informal Network Bias

A fourth lesson from the research team's review of the literature is that the channel through which individuals receive information can affect

---

[19] Brian Uzzi, "Embeddedness in the Making of Financial Capital: How Social Relations and Networks Benefit Firms Seeking Financing," *American Sociological Review*, 1999; Ray Reagans and Bill McEvily, "Network Structure and Knowledge Transfer: The Effects of Cohesion and Range," *Administrative Science Quarterly*, Vol. 48, 2003, pp. 240–243.

the degree of uptake and the ultimate quality of decisionmaking. Studies suggest that the use of personal sources (i.e., informal conversations within one's network) improves strategic decision quality. This is because informal connections feed initial problem diagnosis and idea generation by furnishing rich data that might not be covered in regular internal reporting or through other impersonal forums.[20] For instance, start-up businesses that are embedded in larger informal communication networks have a better chance of surviving external economic shocks.[21]

This reiterates a key distinction we discussed earlier in this chapter between formal reporting structures and procedures and informal practices and relationships for facilitating communications both within and across organizations. Formal channels include official newsletters, memoranda, and other communications based on an organization's authority structure. VOLTS and CIPs are examples of this kind of communication between acquisition and intelligence. Informal channels refer to the typically unofficial communications that occur through casual social contacts.[22] Conversations between intelligence and program staff that build relationships that are later used to share information are an example of informal communications. To quote one landmark study of this dynamic, "If the formal organization is the skeleton of the company, the informal is the central nervous system driving the collective thought processes, actions, and reactions of its business units."[23] While informal networks are associated with several pathologies—such as lack of communication within or between departments, overreliance on single points of failure, and self-aggrandizement among

---

[20] Wolfgang Ganswein, *Effectiveness of Information Use for Strategic Decision-Making*, Gabler, 2011, pp. 220–221.

[21] Ornit Raz and Peter A. Gloor, "Size Really Matters—New Insights for Start-Ups' Survival," *Management Science*, Vol. 53, 2007, pp. 169–170.

[22] Guowei Jian, "Informal Communication and the Grapevine," in *Encyclopedia of Management Theory*, 2013.

[23] David Krackhardt and Jeffrey R. Hanson, "Informal Networks: The Company Behind the Charts," *Harvard Business Review*, Vol. 71, 1993, p. 104.

power-hungry individuals—they can still be recognized, analyzed, and used consciously to improve communication across organizations.[24]

Lessons Learned for Intelligence Support Processes

In practice, informal networks provide important avenues for personal and professional development through information exchange.[25] Employees rely on personal contacts for many contingencies, from meeting impossible deadlines to getting advice on strategic decisions to finding out the truth about a new boss.[26] Therefore, this information exchange is likely to pick up when the subject is of particular importance to the speaker and the circumstances are highly ambiguous, whether because formal communications are unclear or because of general conditions of organizational uncertainty.[27] This suggests that individuals lean into their informal connections when they lack other viable sources of information or guidance or when they are under stressful circumstances—as we observed among acquisition personnel who obtained answers to time-sensitive questions from contacts in the intelligence community. In this way, researchers generally agree that these networks often facilitate beneficial outcomes, such as improving organizational efficiency, reducing anxiety, making sense of limited information, identifying pending problems, and signaling early warning of organizational change.[28] Further, they are a key source of social

---

[24] Keith Davis, "Management Communication and the Grapevine," *Harvard Business Review*, Vol. 31, 1953, p. 43.

[25] Rob Cross and Robert Thomas, "A Smarter Way to Network," *Harvard Business Review*, Vol. 89, 2011, pp. 149–150.

[26] Rob Cross and Laurence Prusak, "The People Who Make Organizations Go—or Stop," *Harvard Business Review*, Vol. 80, 2002, p. 105.

[27] Gordon W. Allport and Leo Postman, *The Psychology of Rumor*, Henry Holt, 1947; S. M. Crampton, J. W. Hodge, and J. M. Mishra, "The Informal Communication Network: Factors Influencing Grapevine Activity," Public Personnel Management, Vol. 27, 1998, pp. 570–573.

[28] R. Brody, "Gossip: Pros and Cons," *USAIR Magazine*, November 1989.

cohesion, which we have already identified as critical for knowledge transfer within networks.[29]

Informal networks also can comprise knowledge repositories or "communities of practice," which are defined as (usually unofficial) in-house networks of experts among whom ideas tend to flow. Whether at private firms or government organizations, these communities can serve many purposes, such as providing research services and knowledge stewardship, setting organizational goals and long-term plans, and fostering peer-to-peer collaboration.

Communities of Practice

An example of a community of practice comes from the United Nations, which established a dozen of these communities to address major social and economic problems in India. Dubbed the Solution Exchange, it enables information sharing between grassroots implementers at the nongovernmental organization level and policymakers at the governmental or development agency level on issues such as nutrition, education, and HIV/AIDS prevention. This arrangement allows practical insights from the field to influence policy design and increase program efficacy by cutting through institutional barriers that otherwise exist due to funding, organization, or location.[30] Maximizing the impact of these communities, however, requires some level of accountability and management oversight, including dedication of time and resources to community participation (especially through face-to-face events); training for community leaders on how to find pockets of expertise and engage new members; and the availability of basic communications technology such as discussion forums, document libraries, and online meeting or chat functionality.[31] TWGs and TSGs could be considered "communities of practice" and could be incentivized to serve a broader purpose than is currently the case.

---

[29] Robert A. Baron and Jerald Greenberg, *Behavior in Organizations: Understanding and Managing the Human Side of Work (Vol. 1)*, Allyn & Bacon, 1990.

[30] Richard McDermott and Douglas Archibald, "Harnessing Your Staff's Informal Networks," *Harvard Business Review*, Vol. 88, 2010, pp. 85–87.

[31] McDermott and Archibald, 2010, pp. 88–89.

Interactions Between Formal and Informal Networks

While brokers are the essential link in the information chain, studies estimate that there are relatively few of them in any given organization—typically, no more than 10 percent of members both send and receive information.[32] By contrast, most individuals merely exist on the periphery of networks, potentially providing or receiving expertise but not participating in information flows otherwise. This means that a small number of individuals is responsible for much of the knowledge transfer that occurs, which may make it easier for formal structures to better monitor, incorporate, and target these networks when sharing official communications.[33]

Here again is where DoIs could be a key enabler. Information sharing across informal networks might also be improved through employee self-evaluations regarding the extent to which they seek out people within or outside of their functional areas; the degree to which hierarchy, tenure, and location matter in terms of who their connections are and whom they seek out; the length of time they have known their connections; and the share of their personal networks that have developed through formal, scheduled interactions versus ad hoc encounters.[34] A periodic, self-conscious examination of their own networks could help acquisition and intelligence personnel better recognize whom they know, where potential gaps are, and how to address them.

Indeed, the interaction between formal structures and informal coordination practices is critical for generating and sharing knowledge through delegation of responsibility, deconstruction of problems, and awareness of dependencies. For team-based projects, formal structures are important for mapping out how personnel with various functional specialties might be paired up (such as embedding an intelligence analyst with a program office), but informal coordination is how work

---

[32] Davis, 1953; Keith Davis, "The Care and Cultivation of the Corporate Grapevine," *Dun's Management Review*, Vol. 62, 1973; H. Sutton and L. W. Porter, "A Study of the Grapevine in a Governmental Organization," *Personnel Psychology*, Vol. 21, 1968; Jian, 2013.

[33] Jian, 2013.

[34] Cross and Prusak, 2002, p. 112.

within and across those teams actually gets done (by connecting that program to the wider IC).

Findings and Recommendations

Formal and informal information flows between the acquisition and intelligence communities are dense, but they are used differently by different individuals and organizations. Formal communications channels depend on digital task registration and management systems and the availability and accessibility of classified communications systems. The complexity of the tasking system and the general lack of availability of classified communications mean that considerable communication between the communities takes place through informal means. Stakeholders generally prefer these informal mechanisms, because they produce timely results. Communications effectiveness cannot be measured, however, and the information that flows between individuals and organizations cannot be discovered and used by other stakeholders.

No single, overarching process exists for determining and codifying a program's threat intelligence needs, levying production requirements for meeting those needs, and then sharing threat information with the program and potentially with others interested in the analysis. Absent a list of priority requirements, the effectiveness of intelligence support to any individual program is difficult to assess. Intelligence producers also have no official basis on which to plan and synchronize production to support programs. This situation could result in analytic organizations underestimating how much acquisition-related intelligence they need to produce. It can also help to explain the difficulty the acquisition community faces when competing for intelligence attention with policy and warfighter stakeholders.

Acquisition programs are generally satisfied with their assigned intelligence support officers, who manage the flow of intelligence requests and products to and from the program office. Program management reported varying levels of intelligence support, with intelligence-sensitive program personnel often describing tight connections with frequent sharing of threat information, and staff from other programs

indicating much less insight into the threat (and indicating that in any case, if the threat necessitated changes, these would have to be driven by and funded by the requirements community/resource sponsors). TL, VOLT, and technical databases are used, but are not cited as the most useful intelligence inputs. TL was generally viewed favorably by interviewees. It is seen as sufficient for less specific threats and for providing information for VOLT. Although it is sometimes customized to particular programs, it falls short in when interviewees need more granular intelligence to support a program or when acquisition leaders see TL as a way to check a box before moving forward. Views on the utility of the VOLT are mixed. Some interviewees find it useful, while others say it is insufficiently detailed to be of great utility. By contrast, program officials value the intelligence production that results from interaction with the intelligence staff and the ad hoc products that result from that cooperation. Both communities highly value informal communications and prefer them over formal channels of communication.

The ability of the intelligence and acquisition communities to share information is encumbered by the lack of personnel clearances for intelligence and compartmentalization of program information into SAPs that are not available to intelligence support officers and analysts. These problems are further aggravated by the paucity and location of classified communications systems available to program offices.

Finding: There is no single, overarching demand signal for intelligence to support acquisition. Some program offices do not develop or maintain sets of priority intelligence requirements or intelligence frameworks that identify enduring threat intelligence needs for their programs. As a result, intelligence tasks are transactionally identified and managed by acquisition intelligence officers. They flow through formal and informal channels but are not codified in any single tasking system. The result is that there is no single "demand signal" for intelligence to support acquisition. The absence of a demand signal makes it difficult to comprehensively effectively assess intelligence needs to support planning and programming and to assess whether intelligence support is satisfying consumer needs.

Recommendation: AFMC should work toward the establishment of a demand signal repository for acquisition-related intelligence, which would serve to more effectively share information, alert intelligence producers to forthcoming intelligence tasks, and provide the hard data necessary to intelligence planning and resourcing. Processes could be established in operational manuals in which formal and informal intelligence tasks could also be cataloged. This repository need not be a new digital tool. It could leverage and evolve existing tools, especially COLISEUM, to serve this purpose. Tasking systems such as COLISEUM are used to manage intelligence production tasks; PEOs and program offices, however, do not establish sets of priority intelligence requirements that serve to guide and prioritize intelligence production over time. Intelligence products responding to program requests can generally be characterized as ad hoc support, as there is no discernible "theme" to any program's intelligence requests. AFMC and AF A2/6 could initiate these changes by interacting with the COLISEUM user group to articulate a vision that could help guide near- to medium-term COLISEUM evolution. Changes required should be aimed at improving COLISEUM's knowledge management to connect requests and answers between similar programs, update its search function algorithms, and exploit artificial intelligence as much as possible to assist with analysis both within and between programs. Additionally, AFMC and AF A2/6 should advocate for the revision of the COLISEUM user's guide, which has not been updated since 2008. Updates should include fresh guidance on standards on entering data into the system and on registering and managing tasks. These changes would enhance the use of COLISEUM as a demand signal repository for acquisition-related intelligence.

Additionally, to help intelligence producers develop PoAs, DoIs could identify sets of priority intelligence requirements at their PEOs (or even at the program level). This would serve to guide and prioritize intelligence collection and analysis so that key acquisition intelligence needs would be met. Another possible approach that is already working for one program would be to use a memorandum of understanding (MOU) between the program office and the intelligence staff outlining program needs and providing SCIF facilities in which intelligence

staff can work alongside program officers. Intelligence staff would also have access to program SAP information to refine the identification of intelligence needs and gaps.

The acquisition and intelligence communities also must address their need for additional intelligence to evaluate (1) long-range developments and (2) the potential of adversaries to suddenly introduce disruptive technologies. To craft a broad requirement for this kind of intelligence, DoIs could utilize their positions to identify these kinds of requirements and package them into a single set of priority intelligence requirements. Identifying the requirements and information gaps would highlight the need for such products, likely including the requirement for experts not currently available in the IC and for additional people, funding, and other resources.

Finding: Communication, collaboration, and coordination between acquisition and intelligence occurs in formal and informal channels, but the informal channel appears to be the most frequently used and currently the most effective means of information sharing. This finding is closely associated to the finding above noting the absence of a comprehensive demand signal for intelligence. Using the informal system produces quicker results and requires less processing time (and less oversight). This approach, however, prevents the formation of broadly available understanding of intelligence availability and inhibits sharing information more broadly; it can also produce duplication of effort and thus not effectively support future planning of intelligence production and expertise.

Providing incentives and opportunities for members of different organizations, or functional groups within the same organization, to develop cohesive and wide-ranging ties with their colleagues appears critical for fostering knowledge sharing. These incentives and opportunities exist to some extent for acquisition and intelligence, but more frequent and regular opportunities to convene these communities and make connections could contribute to greater cohesion and range in their personal relationships.

Recommendation: While the variety and density of formal and informal communications channels provides sufficient capa-

bility to share information, a better understanding of all intelligence transactions, especially the informal ones, would enhance information sharing, preclude duplicative tasks, and allow intelligence managers to better assess and potentially improve the effectiveness of intelligence provision to the acquisition community. Our interviews suggest that the TWG could be more effectively leveraged both to communicate and to build trust between the communities. We were surprised that interviews with intelligence and acquisition personnel spent little time discussing TWGs; these forums exist but may not be taken advantage of in a way that maximizes their potential utility. According to interviews, TWG meetings include intelligence and program personnel at the working level and include a broad range of discussions about the program status, including intelligence needs. TWGs were frequently mentioned by interviewees as both a forum for identifying and codifying intelligence requirements but also as opportunities that promoted relationship and trust building between program offices and intelligence support staffs. TWGs should be used more frequently and more effectively to communicate key information, increase the transparency between the communities, and to generate trust. Transparency could also help intelligence officers understand how program offices can best absorb intelligence data. While intelligence databases are designed to be used by consumers to "pull" intelligence, few nonintelligence offices have the training or systems from which to conduct intelligence pulls, making it all the more important for intelligence officers to be sensitive to common intelligence needs and to share information widely. In addition to the exchange of program and intelligence information, TWGs could be used to discuss personnel security clearances and to build a stronger case for secure facilities to host sensitive discussions, including SCI and SAP material.

Additionally, the establishment of DoIs around the Air Force acquisition community is another opportunity to cultivate relationships that will improve the climate for information exchange. SMEs from program offices told us that assigning the DoIs directly to the program staff (instead of to an offsite intelligence office) should allow for stronger relationships to be developed and that nonintelligence program elements would have greater "trust" in their intelligence coun-

terparts. Recognizing, encouraging, incentivizing, and routinizing these exchanges would be a key step toward a better-integrated materiel intelligence enterprise. DoIs are well positioned to improve communications between the communities and could be especially useful in exploiting the informal networks that appear to be the preferred method of communication.

Finding: Intelligence and acquisition personnel often lack the proper clearances to facilitate information sharing and appropriate facilities in which to review and use classified material. Intelligence generally works at the TS and SCI levels. An insufficient number of acquisition officers have these clearances, however, and are denied access to vital threat information. Similarly, while acquisition officers are often cleared for SAP programs, which contain the most sensitive performance-related information about the equipment, intelligence support officers are not cleared for these SAPs. Without access to system performance data, intelligence analysts are unable to provide targeted intelligence analysis to program technical personnel. Program staff need TS and SCI clearances to ensure they can access the most sensitive threat data available to the IC. Intelligence staff need the proper clearances and access to SAP information to reduce stovepiping and ensure that intelligence personnel are informed and writing threat-informed intelligence products. Ensuring an adequate number of SCI and SAP clearances, however, will not be effective unless more facilities are created where these materials can be received, retained, and discussed.

Recommendation: Improvement in the *content* of what is shared needs to be achieved. More SCI clearances need to be obtained for program personnel who can benefit from access to more sensitive and detailed intelligence. Alternatively, a way may be sought to downgrade highly classified material to make it accessible to more people or to extract less-classified insights from TS SCI material. Similarly, additional SAP clearances need to be made available to intelligence staffs to improve their detailed understanding of U.S. capabilities so that intelligence-threat information can be refined and add value to the program office. More of both kinds of access will not be useful unless

the numbers of facilities accredited for these materials are increased. One idea would be to dual accredit facilities SCIFs for SAP access and develop unique protocols for how each facility would be used to ensure the security of the SAP material. Clearances and facilities are not cost free; one way to fund them would be to tax programs for the funds and try to make facilities available and convenient for those programs that were taxed.

Additionally, one way to reduce barriers across similar programs would be to put all programs under the same level of SAP access, thereby giving all personnel with SAP access to all programs in the portfolio. This could be followed up by convening meetings to update all SAP access personnel on the progress of each program. Of course, this defeats the purpose of greatly minimizing access to SAP material, so this reflects an inherent trade-off between the risk of not having access when someone has a compelling need to know and the risk of exceptionally grave damage to national security through exposure of highly classified material.

CHAPTER FIVE

Workforce Analysis

Introduction

Workforce development within the acquisition intelligence career fields is one of the areas where intelligence and acquisition intersect. Interviewees expressed concerns about whether the staffing, training, and expertise for the field is sufficient to support acquisition programs. In this chapter, we provide a focused scoped workforce analysis (versus a comprehensive manpower study) to answer specific research questions that would help us determine whether the existing staffing, training, and expertise in these fields are sufficient to support the USAF acquisition mission.

The goal of this workforce analysis was to establish the following baselines: (1) size of the USAF's acquisition intelligence organization, (2) necessary capabilities and expertise to support the USAF acquisition mission, (3) career stability required to recruit and retain the necessary capabilities and expertise, and (4) types of available training for acquisition intelligence personnel. These baselines should help determine how best to organize existing acquisition intelligence personnel, as well as other personnel with the necessary expertise, to provide optimal support for the USAF acquisition life cycle.

For the purposes of this inquiry, acquisition intelligence organizations are those units in USAF that support the acquisition mission by establishing guidance and employing the operational workforce across the entire acquisition life cycle; acquisition intelligence personnel are

civilian and military intelligence personnel assigned to acquisition intelligence organizations.[1]

Current Accounting and Distribution of Acquisition Intelligence Personnel Supporting the Air Force Acquisition Mission

To determine the size of the USAF acquisition intelligence organization, we captured data for authorized and assigned intelligence civilian and military personnel in the USAF Active Duty (AD), Air National Guard (ANG), and Air Force Reserve (AFR) components.[2] Our data included intelligence officers (14N) and enlisted personnel (1N) Duty Air Force Specialty Codes, respectively, as well as civilian intelligence analysts with 0132 Occupation Codes within the organizations listed in Table 5.1.

This list is consistent with the Institute for Defense Analyses' 2018 study *Military Department and Service Acquisition Intelligence Workforce.* We excluded HQ USAF and included 14th IS, the AFR classic associate unit that has integrated with the 21st IS to support the acquisition mission, because our detailed analysis focused on the implementing commands (AFMC and SMC). Additionally, we excluded contractor and intern personnel from our data analysis, because we used the Military Personnel Database System (MilPDS) as our primary data source. We do, however, discuss different sources for new hires in the "Career Field Management" section below.

---

[1] We excluded the contractor data from our study because of on the results of a previous study the Institute for Defense Analyses conducted in 2018: P. Lowell, Tiki Mitchell, Marc Luoma, and Vivian Cocca, *Military Department and Service Acquisition Intelligence Workforce*, Institute for Defense Analyses Project 4468, August 21, 2018. This study showed that the contractor workforce did not represent a significant proportion of the overall acquisition intelligence personnel force.

[2] Our data excluded contractors, Federally Funded Research and Development Center employees, and intern personnel. FY2019, or September 30, 2019, was the cut-off date for our datasets.

Table 5.1
Acquisitions Intelligence Organizations Performing Acquisition Intelligence Functions

Acquisition Intelligence Implementing Organizations	Other Supporting Organizations
AFRL AFMC/A2 AFLCMC/IN • 21st IS • AFLCMC/INB (Intelligence, Tinker Air Force Base [AFB], Oklahoma) • AFLCMC/ING (Intelligence, Robins AFB, Georgia) • AFLCMC/ING-OL (Intelligence, Robins AFB, Georgia, Operating Location) • AFLCMC/INH (Intelligence, Hanscom AFB, Massachusetts) • AFLCMC/INH-OL (Intelligence, Hanscom AFB, Massachusetts, Operating Location) • AFLCMC/INL (Intelligence, Hill AFB, Utah) • AFLCMC/INM (Intelligence, Eglin AFB, Florida) AFNWC Air Force Sustainment Center AFIMSC (Air Force Installation and Mission Support Center) AFTC • AEDC (Arnold Engineering and Development Center) • 412th Test Wing • 96th Test Wing SMC/IN AFSPC/A2 14th IS Air Force Reserve (AFR)	*Policy* • SAF/AQ • AF/A2/6 *Operations/Requirements* • ACC/A2 • AMC/A2 • AFWIC *Air Force Intelligence Production Center* • NASIC *Independent Tests* • AFOTEC

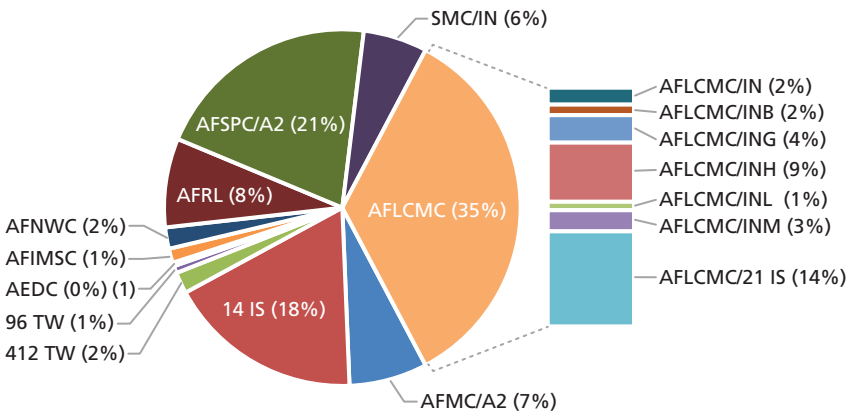
We found a total of 310 intelligence personnel across the acquisition Intelligence organizations at the end of fiscal year (FY) 2019. AFSPC/A2, had the highest single organization concentration (at 21 percent) of acquisition intelligence personnel. Approximately 21 percent of the personnel were also distributed among the ININ that support various AFPEOs and AFSC. The 14th IS had the second highest single organization concentration (at 18 percent), and the 21st IS had

the third highest concentration (at 14 percent). The remainder of the acquisition intelligence capabilities support research and development (AFRL), test and evaluation (AFTC, AEDC, 412th Test Wing [TW], 96th TW), space and nuclear weapons acquisition (AFNWC, SMC/IN), and other supporting functions (AFIMSC). Figure 5.1 below shows the complete distribution of intelligence personnel across the acquisition intelligence organizations.

Furthermore, as Figure 5.2 illustrates, military personnel make up the majority of the intelligence workforce at these organizations; most of those are officers.

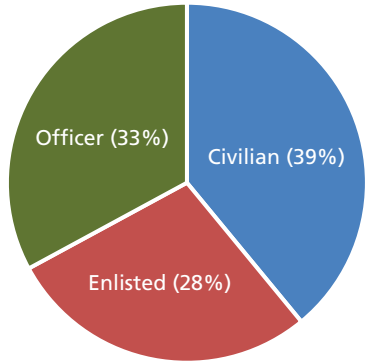
Finally, as Figure 5.3 demonstrates, the intelligence workforce is staffed (assigned personnel) at almost 99 percent of the current career field demand (authorizations). The intelligence career field at the given organizations was understaffed by four personnel at the end of FY2019. Further analysis will explore where these staffing shortfalls are and whether they can be mitigated by rebalancing the intelligence workforce.

Figure 5.1
Accounting and Distribution of Intelligence Personnel Supporting the Acquisition Mission



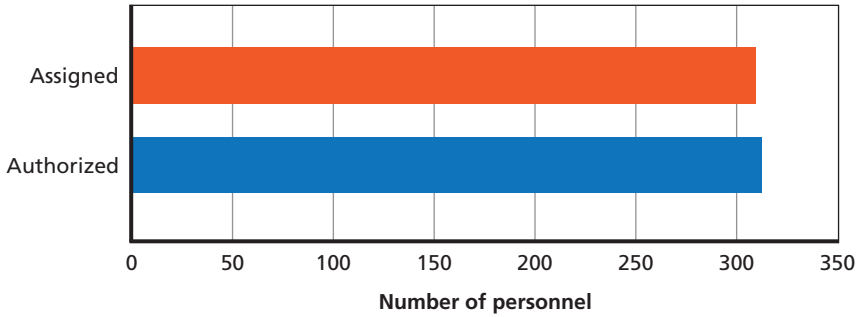
SOURCE: RAND analysis of MilPDS data, FY2019.
NOTE: Data captured included AD, ANG, and AFR personnel. However, we did not find any ANG personnel assigned to these acquisition intelligence organizations. Data includes currently assigned intelligence civilian, enlisted, and officer personnel.

Figure 5.2
Corps Composition of Intelligence Personnel Supporting the Acquisition Mission



SOURCE: RAND analysis of MilPDS data, FY2019.

Figure 5.3
Intelligence Workforce Staffing at Acquisition Intelligence Organizations



SOURCE: RAND analysis of MilPDS data, FY2019.

This section examines a snapshot of the USAF intelligence workforce supporting the acquisition mission at the time of this report. Further sections analyze elements of this data (e.g., AFSC, occupation code, and corps) over time to understand whether staffing has been trending upward or downward or remained constant over time.

Opportunities for Rebalancing

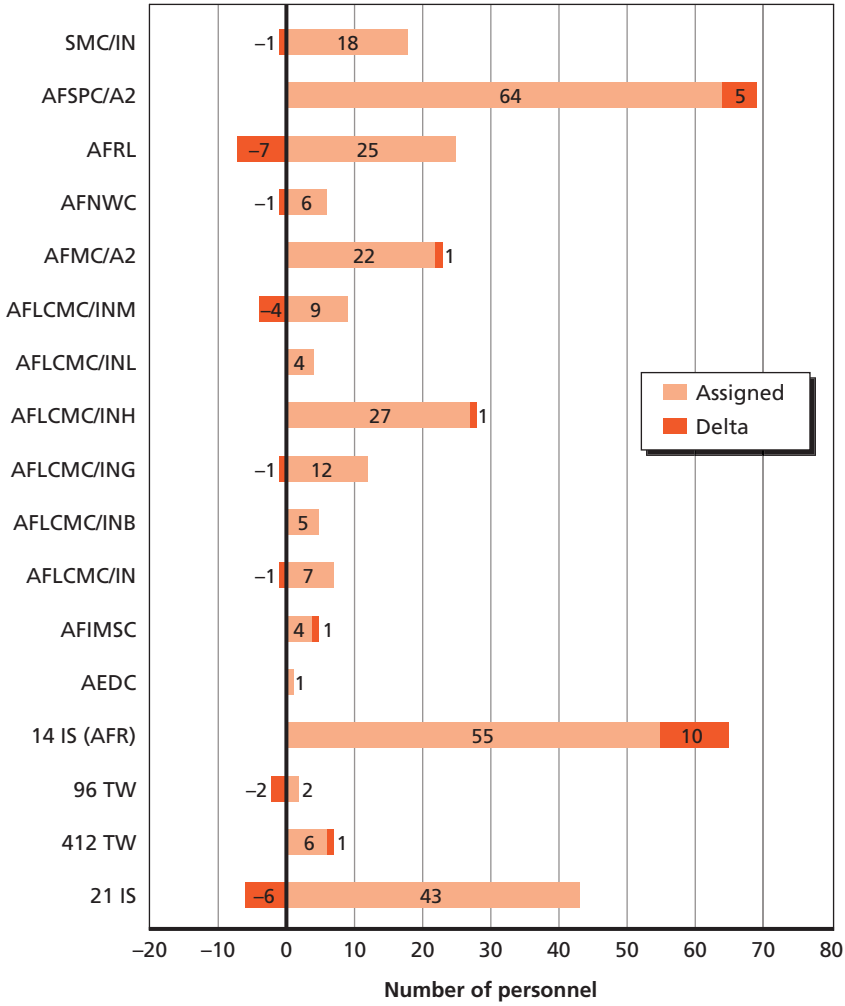
The state of the intelligence workforce does not provide much opportunity to rebalance existing personnel from overstaffed units (where assignments are higher than authorizations) to understaffed units (where assignments are lower than authorizations). Figure 5.4 illustrates that at the end of FY2019, eight units were understaffed by a total of 23 personnel; six units were overstaffed by a total of 19 personnel; and three units were staffed according to their demand. Rebalancing will still leave this workforce understaffed by a net of four personnel.

Opportunities for rebalancing also depend on several workforce requirements. First, what is the feasibility of transferring intelligence personnel from overstaffed to understaffed units? For example, the 14th IS is overstaffed by ten personnel; however, these personnel belong to the AFR, whereas the majority of vacancies are in AD units. Other difficulties for rebalancing may involve swapping between different ranks, enlisted personnel AFSCs, and civilian and military billets. Each case may require billet conversion or recoding before any rebalancing is possible. Second, what are the specialties and skill-level requirements for the vacant positions to ensure rebalancing is feasible? There could be shortages in civilian staffing and a surplus in military staffing, making rebalancing the workforce less feasible. Third, what is or should be the desired ratio of junior to senior intelligence personnel in a unit? Senior personnel might be easier to hire, but their experience might not be consistent with the needs of the acquisition mission.[3]

This analysis was based on a snapshot of data to illustrate one way to view and mitigate current workforce shortfalls. Further analysis of the issue of understaffing in this workforce below examines the trends in authorizations and assignments across specific AFSCs and occupation codes.

[3] Lowell et al., 2018, p. 17.

Figure 5.4
Opportunities to Rebalance Intelligence Workforce in Acquisition Intelligence Organizations



SOURCE: RAND analysis of MilPDS data, FY2019.

Intelligence Personnel Supporting Air Force Program Executive Offices

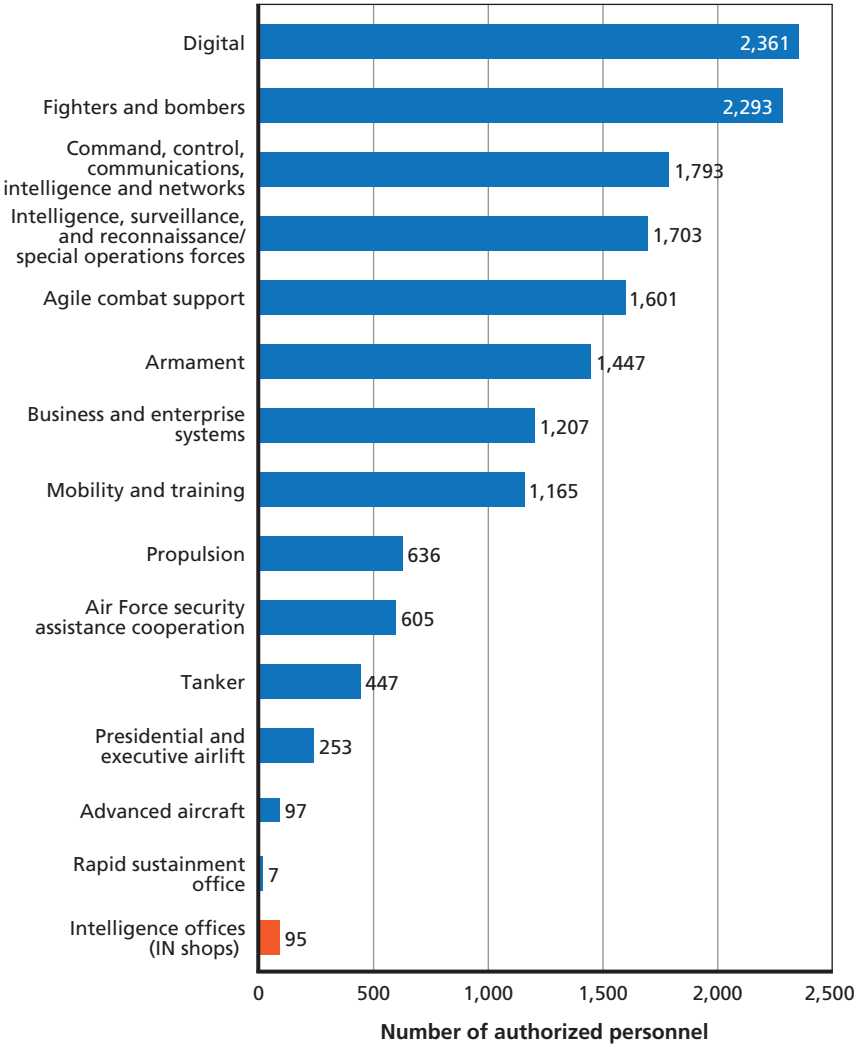
The above analysis summarized the state of the intelligence workforce at the acquisition intelligence organizations prior to FY2019. AFMC/A2 has been reorganizing its intelligence workforce to improve acquisition intelligence support to all USAF acquisition programs. Specifically, AFLCMC/IN began to embed DoIs and intelligence analysts within AFPEOs for closer and more targeted support to these organizations. Since AFLCMC still maintains the billets identified for transfer to PEOs (and included in the above analysis), the data we captured to describe personnel requirements at the AFPEOs do not reflect any intelligence personnel. The data captured and subsequently presented in Figures 5.5 and 5.6, however, aim to show the contrast between nonintelligence and intelligence personnel requirements at AFPEOs, as well as between intelligence personnel requirements and the volume of programs they are expected to support.

Figure 5.5 shows the current demand (authorizations) for personnel in AFLCMC/IN offices and respective PEOs for March 2020. While this data also included nonintelligence AFSCs (increasing the number from 69 to 95 for AFLCMC/IN's total), this depiction underlines the stark difference between the personnel requirements at AFPEOs (15,615 personnel) and the number of personnel in intelligence shops, including intelligence and nonintelligence personnel, tasked to support them (95 total personnel, including 69 intelligence personnel).

Figure 5.6 represents the volume of acquisition programs at AFLCMC that intelligence personnel assigned to AFLCMC intelligence offices currently support. At the end of FY2019, 64 intelligence personnel were supporting 985 acquisition programs across 12 different AFPEOs. Additionally, six intelligence personnel were supporting 64 programs at AFNWC,[4] and 18 additional intelligence personnel were supporting 64 programs at SMC/IN.

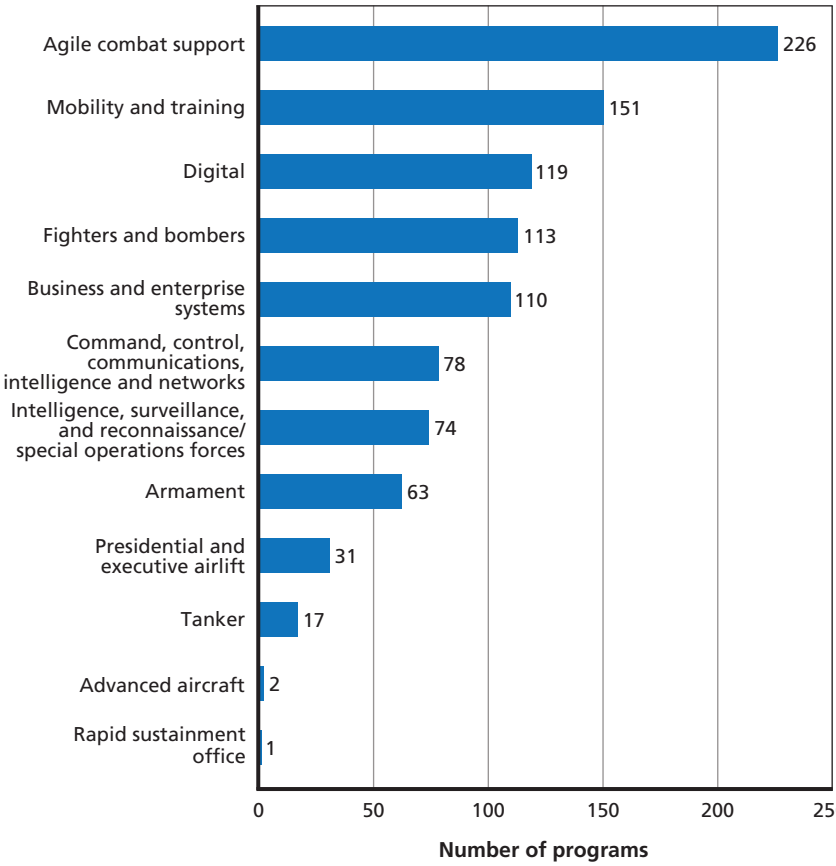
[4] According to correspondence with AFNWC's Intelligence Division, AFNWC also has an additional five personnel (for a total of 11 personnel) performing acquisition intelligence support to the 64 programs. These personnel are a mix of civilian engineers and scientists and military engineers.

Figure 5.5
Size of the Intelligence Shops Supporting Acquisition Programs Compared with Size of Programs They Support



SOURCE: RAND analysis of Personnel Accountability System data, March 2020.
NOTE: Program Executive Offices (PEOs) include contracting, engineering, financial, logistics, and program management functions.

Figure 5.6
Volume of Air Force Acquisition Programs Intelligence Personnel Support



SOURCE: RAND analysis of SAF/AQX [Secretary of the Air Force for Acquisition Integration], Monthly Acquisition Report data, November 2019.

The data in Figure 5.6 indicate that the workload (i.e., actual work and potential demand) for intelligence personnel across acquisition intelligence organizations varies across AFPEOs. Some interviewees also expressed that they have more meetings for programs to attend than they can support and are often asked to "do less with more."[5]

[5] Interview with AFPEO/Digital on May 6, 2020.

They further noted that while more personnel resources may be needed to support more programs and meetings, the support these personnel would be able to provide would be more comprehensive. Intelligence personnel can also expect to support a variety of programs that require different levels of technical knowledge. The subsequent sections will discuss the capabilities intelligence personnel might need to provide effective support to their acquisition mission.

"All for One"?

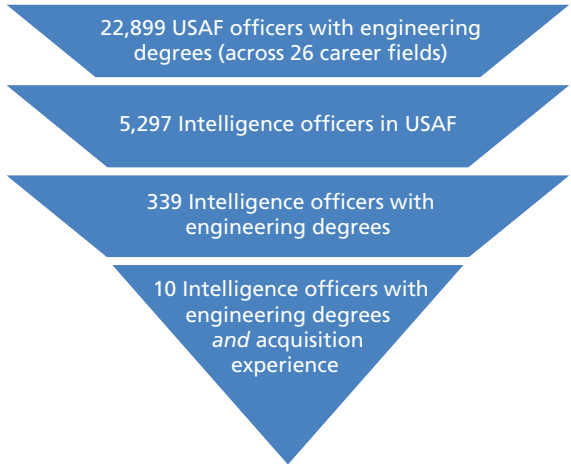
Several interviewees noted that acquisition intelligence is a technical field because of the "exquisite [Scientific and Technical] intelligence [S&TI] required for acquisition decisions." Interviewees further noted that the capability to request and understand this type of intelligence requires basic knowledge of engineering concepts and acquisition processes in addition to intelligence analysis skills.

One of the problems has been finding individuals in USAF with all three attributes. Interviewees further elaborated that the acquisition intelligence community comprises either "great analysts" who have never worked in acquisition or engineers who have limited "personal skills." Our subsequent analysis aimed to examine whether or not USAF produces this capability and, if it does, where the capability resides. Due to the desire for the intelligence analyst to have a college degree and background in acquisition, an officer career field, we limited our inquiry to USAF officers only. (Subsequent sections will discuss the civilian acquisition intelligence workforce in more detail.) First, we looked at how many intelligence officers in USAF have an engineering degree (ED). As Figure 5.7 illustrates, we found 339 intelligence officers with EDs out of a total 5,297 intelligence officers in the USAF, or approximately 6.4 percent (339/5,297).[6] The USAF has a Tier 1 mandatory target accession rate of 30 percent for intelligence officers with education backgrounds in computer and information sciences, engineering, mathematics and statistics, or physical sciences.[7] It

[6] These data include ADuty, AFR, and ANG personnel.

[7] U.S. Department of the Air Force, "Air Force Officer Classification Directory (AFOCD): The Official Guide to the Air Force Officer Classification Codes," Air Force Personnel

Figure 5.7
Breakdown of Intelligence Officers with Engineering Degrees and Acquisition Experience



SOURCE: RAND analysis of MilPDS data, FY2019.

is unclear whether USAF is achieving its requirement for intelligence officers with EDs at the current level of 6.4 percent.

Furthermore, all officers with EDs are currently distributed across 26 career fields. Certain career fields in USAF, such as civil engineering and developmental engineering, require an ED.[8] One RAND study also showed that officers with EDs are more likely to request an assignment in an engineering-related career field and that USAF is likely to grant that request.[9] The intelligence career field does not require an ED, however, and contains the tenth highest percentage of ED accessions (i.e., tenth in priority for EDs for USAF out of the 26 career fields) at approximately 1.5 percent (339/22,899 ED holders in USAF).

Center, April 30, 2020a, p. 259.

[8] U.S. Department of the Air Force, 2020, pp. 264, 268.

[9] Lisa M. Harrington, and Tara L. Terry, *Air Force Officer Accession Planning,* Santa Monica, Calif.: RAND Corporation, RR-1099-AF, 2016.

Second, we looked at how many intelligence officers with EDs also have acquisition experience. We captured data that listed these officers' primary, secondary, and tertiary AFSCs as 63X (Acquisition).[10] We found ten intelligence officers with this background, or approximately 0.2 percent (10/5,297) of intelligence officers in USAF. Only one of these officers was assigned to an acquisition intelligence unit: 14th IS (the AFR unit).

Finally, we also examined how many acquisition officers (63X Duty AFSC) with EDs also have past intelligence experience (either as a primary, secondary, or tertiary AFSC), as these officers will have received formal training in USAF intelligence activities and completed a three-year tour in the intelligence field. We found 35 officers with this background assigned across 16 organizations; 16 of the officers were assigned to acquisition intelligence organizations (AFLCMC, AFRL, AFTC, and SMC). The acquisition career field holds the eighth highest percentage of ED accessions (i.e., eighth in priority for EDs for USAF) at approximately 2.8 percent (649/22,899 ED holders in USAF), which is slightly higher than that for the intelligence career field.

In all, our analysis confirmed interviewees' statements that a relatively small number of USAF officers (45: ten intelligence and 35 acquisition) have the background in intelligence activities, engineering concepts, and acquisition processes desired by the acquisition intelligence community. We further found an even smaller number of these officers (17 total, which included one intelligence and 16 acquisition professionals) to be assigned to acquisition intelligence organizations.

These numbers seem low when compared with the overall number of intelligence personnel (310) assigned to these organizations; and the desired capability resides primarily outside of the acquisition intelligence community. Furthermore, intelligence officers with these capabilities in these organizations are more likely to complete their tour in acquisition intelligence and move on to other intelligence assignments. It is more likely to find acquisition officers with these same capabilities in acquisition intelligence, as these officers will remain engaged in

[10] Duty AFSC indicates a position to which the officer is currently assigned; primary AFSC indicates the current AFSC; secondary and tertiary AFSCs indicate past assignments.

acquisition. (For a more detailed discussion on how these officers can attain all three attributes, refer to the "Career Field Management" section below.)

"One for All"?

Some interviewees recognized that they will not always have intelligence personnel with the expertise that "we in acquisition need" and mentioned using another approach to conducting acquisition intelligence—namely, matching intelligence personnel and engineers in teams to provide more appropriate program support. We further investigated personnel data for scientists, engineers, and acquisition (S/E/A) professionals within acquisition intelligence organizations to assess the availability of additional expertise that supports the acquisition mission.

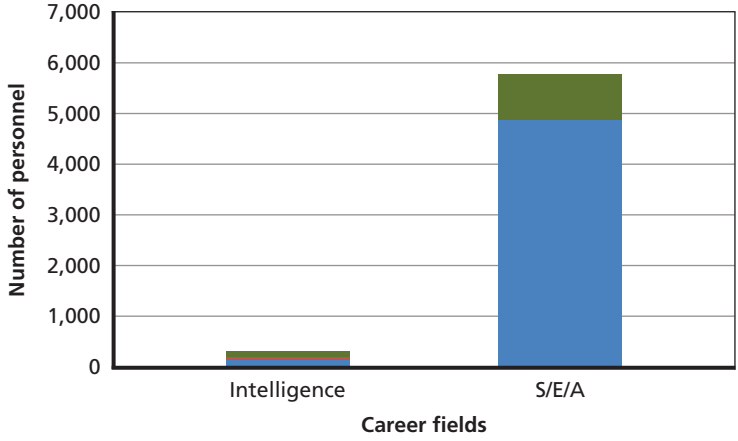
Figure 5.8 demonstrates the number of S/E/A personnel across the acquisition intelligence organizations compared with the number of intelligence personnel. The S/E/A workforce is significantly larger than the intelligence workforce. The S/E/A workforce is also predominantly civilian.

As Figure 5.9 illustrates, however, the S/E/A workforce is also understaffed.

Scientific, Engineering, Acquisition, and Intelligence Workforce Historical Trends

Figures 5.10 and 5.11 illustrate trends in the S/E/A and intelligence civilian and military communities over the last decade. Almost 95 percent of this combined workforce are S/E/A professionals. The majority of the workforce is civilian, while most of the intelligence workforce is military (see Figure 5.2 above). Figure 5.10 below shows that overall, acquisition intelligence organizations have seen an increase in the total S/E/A and intelligence workforce since 2010. However, only the civilian S/E/A workforce has seen a consistent increase in its authorizations (demand) and assignments (staffing), which suggests that USAF recognizes the importance of science and technology expertise for the acquisition intelligence mission (see upper left of Figure 5.11). The trend for the civilian S/E/A workforce also suggests that USAF has not had

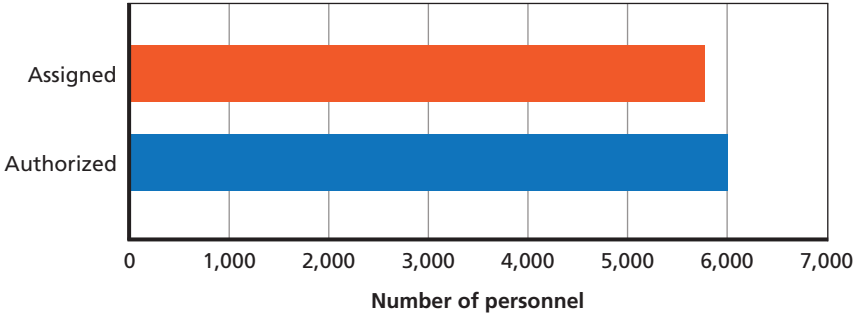
Figure 5.8
Intelligence Workforce versus Scientific, Engineering, Acquisition Workforce



Officer	102	884
Enlisted	87	0
Civilian	121	4,902

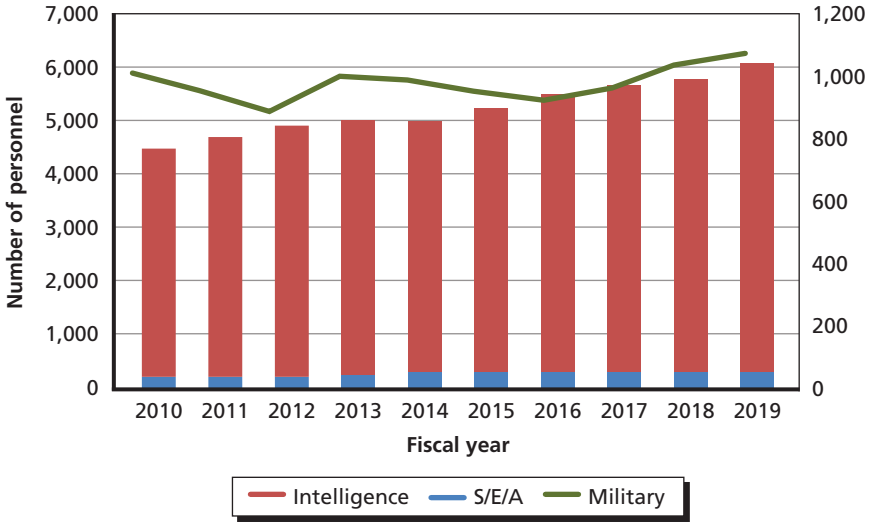
SOURCE: RAND analysis of MilPDS data, FY2019.

Figure 5.9
Scientific, Engineering, Acquisition Workforce



SOURCE: RAND analysis of MilPDS data, FY2019.

Figure 5.10
Growth and Composition of Scientific, Engineering, Acquisition, and Intelligence Workforce



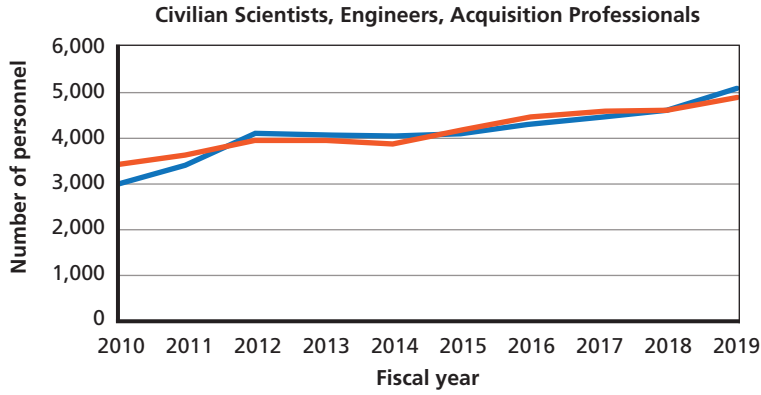
SOURCE: RAND analysis of MilPDS data, FY2019.

difficulty sustaining the staffing in these civilian career fields for the acquisition intelligence mission.

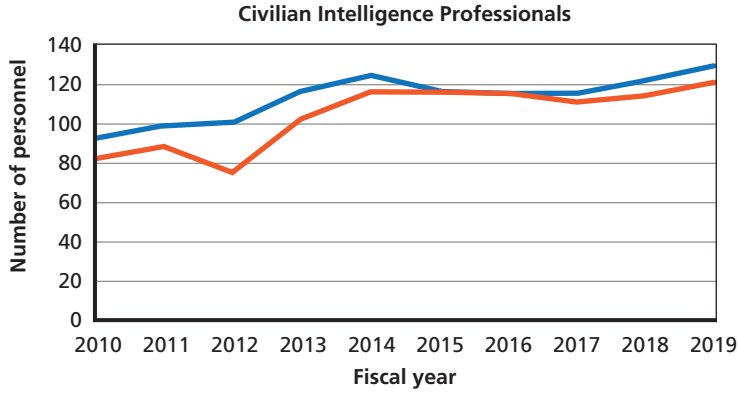
The staffing for the military S/E/A workforce (see upper right of Figure 5.11), on the other hand, has been more difficult to maintain, even as the demand for military S/E/A professionals steadily increased. The same seems to hold for civilian intelligence professionals (see lower left of Figure 5.11), where the demand has been higher than the staffing levels. And the staffing levels for the military intelligence professionals have only recently (since 2017) caught up with their demand (see lower right of Figure 5.11).

Demand for the overall S/E/A workforce increased by a factor of 1.59 between 2010 and 2019, while demand for the overall intelligence workforce increased by a factor of 1.37. The trends in the overall intelligence workforce have also been inconsistent compared with their S/E/A counterparts, which suggests the difficulty of characterizing

Figure 5.11
Comparing Historical Trends for Authorizations and Assignments in Scientific, Engineering, Acquisition Workforce and Intelligence Workforce in Acquisition Intelligence Organizations, 2010–2019

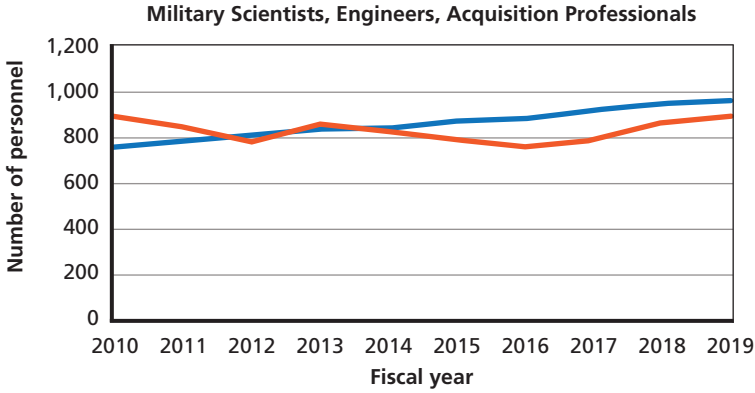


Authorized	3,028	3,435	4,115	4,077	4,063	4,128	4,308	4,485	4,611	5,057
Assigned	3,420	3,650	3,951	3,955	3,892	4,178	4,457	4,603	4,641	4,902

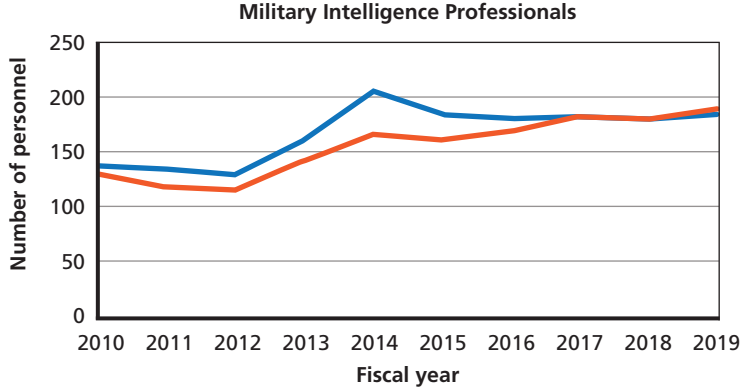


Authorized	92	99	100	116	124	117	115	115	122	129
Assigned	82	88	75	102	116	116	115	111	114	121

Figure 5.11—Continued



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Authorized	758	786	811	839	846	871	889	920	945	963
Assigned	885	846	783	862	827	791	760	792	867	890



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Authorized	137	134	129	162	205	185	180	181	182	185
Assigned	129	117	115	142	166	162	169	182	181	189

SOURCE: RAND analysis of MilPDS data, FY2019.
NOTES: Data captured included AD, ANG, and AFR personnel. However, we did not find any ANG personnel assigned to the acquisition intelligence mission. S/E/A civilians are all permanently assigned; S/E/A military are all officers in AD and AFR units. The majority of Intelligence civilians are permanently assigned, with reserve civilians appearing in 2018–2019; military Intelligence personnel are in AD and AFR units. Civilian authorizations are designed to advertise the position and are updated at the commander's discretion.

the demand for the intelligence workforce and of fulfilling the stated demand over the last decade.

The trends for military personnel and civilian intelligence personnel indicate that establishing a clear demand signal in acquisition intelligence early is key, because it can take more than six years to provide sufficient staffing for these areas. The trends for the military S/E/A and intelligence workforce might also reflect USAF's prioritizing support for the warfighter versus the acquisition mission over the last decade. The trends also suggest that the civilian S/E/A workforce has been the least affected by military operations of the last decade in that USAF continued to recruit and retain civilian S/E/A professionals. This means that pairing intelligence analysts with specific engineers (e.g., experts in reverse engineering) or adding engineers to intelligence teams that provide direct support to acquisition programs could be a viable option for improving intelligence support to the acquisition mission. In addition, civilian engineers are more likely to be proficient in a particular field, because military engineers are more likely to do "engineering management" that requires "technical specialization and an academic degree in a particular specialty."[11]

Training

The U.S. Air Force provides several training opportunities, both in residence and as remote instruction, for intelligence personnel assigned to the acquisition mission. All intelligence personnel assigned to AFMC are currently required to complete the Acquisition IFTU.[12] It is a three-day in-residence course administered by the 21st IS for AFMC/A2 and consists of the learning objectives for DAU's Acquisition Intelligence course (ACQ 110), which are listed in Table 5.2. Between 2016 and 2019, 393 intelligence personnel (military from the AD, AFR, and ANG components; civilians; other agencies; and contractors) com-

[11] U.S. Department of the Air Force, 2020, p. 214.

[12] According to email correspondence with Headquarters Air Force Materiel Command, Intelligence Directorate, Intelligence, Surveillance, and Reconnaissance Forces Division, Workforce Development, the Acquisition IFTU is part of initial qualification training for AFMC Acquisition Intelligence personnel.

pleted the Acquisition IFTU. Only two of the organizations included in this study (AEDC and AFIMSC) did not have anyone go through the Acquisition IFTU in the same time period.[13] AFMC also offers a three-day mobile training course in lieu of IFTU and an executive-level three-hour course focused on specific guidance and familiarization.[14]

On July 30, 2019, OUSD(I&S)'s Human Capital Management Office released a memorandum outlining foundational credential requirements for the prospective "Acquisition Intelligence Career Occupation Program." Acquisition intelligence personnel will need to complete (1) one year in an acquisition intelligence position that is designated by the DoD component Acquisition Intelligence Career Occupation PM; (2) DAU's Fundamentals of Systems Acquisition Management (ACQ 1010, formerly ACQ 101); (3) DAU's Introduction to the JCIDS course (CLR 101); and (4) DAU's Acquisition Intelligence course (ACQ 110).[15] Some individual training centers have separate, additional training requirements for their personnel.

ACQ 1010 is a 13-hour distance-learning course that introduces junior military and civilian personnel new to the DoD acquisition field to the DoD systems acquisition process, JCIDS, the PPBE process, the DoD 5000–series policy documents, and the current issues in systems acquisition management.[16] CLR 101 is a three-hour module that provides an overview of JCIDS: terms, definitions, basic concepts, processes, roles and responsibilities, and JCIDS's interaction with the DAS and PPBE.[17] The ACQ 110 course is specifically geared toward intel-

---

[13] AEDC only had one intelligence analyst, a senior-level civilian, at the end of FY2019. AFIMSC had four intelligence personnel: two midlevel civilians, one senior noncommissioned officer, and one junior officer.

[14] Email correspondence with Headquarters Air Force Materiel Command, Intelligence Directorate, Intelligence, Surveillance, and Reconnaissance Forces Division, Workforce Development.

[15] DoD, 2019.

[16] This course replaced the ACQ 101, Fundamental of Systems Acquisition Management, on May 19, 2020. DAU, Training Center, Training Courses, Courses and Schedules, "ACQ 1010 Fundamentals of Systems Acquisition Management," May 19, 2020.

[17] DAU, Training Center, Training Courses, Courses and Schedules, "CLR 101 Introduction to the Joint Capabilities Integration & Development System," October 16, 2019c.

ligence professionals in acquisitions and requirements communities and provides a "joint service-level overview of Acquisition Intelligence that addresses timely and effective communication between the intelligence, requirements, and acquisition communities throughout the acquisition lifecycle."[18] This six-hour distance-learning course introduces participants to real-life situations to practice decisionmaking and communication with the appropriate offices throughout the acquisition life cycle. Participants also learn about the roles, responsibilities, and activities within the acquisition intelligence workforce, as well as specific military-branch best practices for communication and workflow among members of the acquisition intelligence workforce. Table 5.2 summarizes the course objectives for ACQ 1010 and ACQ 110.

Table 5.2
Acquisition 1010 and 110 Course Objectives

ACQ 1010	ACQ 110
Recognize the key drivers of the DoD's Acquisition Management System	Define acquisition intelligence relationships throughout the acquisition life cycle in accordance with DoDDs and other regulations that regulate acquisition intelligence. Recognize the intelligence sensitivity determination process across the services.
Recognize the Joint Capabilities and Integration Development System is the key driver of new defense acquisition program requirements.	Recognize the intelligence supportability analysis process.
Recognize the key activities and considerations of a phased acquisition.	Recognize the purpose of intelligence requirements analysis.
Recognize the resource allocation process in defense acquisition management.	Recognize the life-cycle mission data plan and intelligence mission data processes in accordance with the DoDD 5250.01 (management of intelligence mission data in DoD acquisition).

[18] DAU, Training Center, Training Courses, Courses and Schedules home page, "ACQ 110 Fundamentals of Acquisition Intelligence," October 30, 2019b.

Table 5.2—Continued

ACQ 1010	ACQ 110
Recognize the importance of cost-estimating techniques, defense budget appropriations, and the budget allocation process in defense acquisition management.	Recall how threat support applies to the acquisition life cycle.
Recognize the significance of the contracting to acquire goods and services in DoD acquisitions.	Recognize the purpose of CIPs.
Recognize that the systems engineering process is used to translate requirements into an integrated, system design solution.	Recognize the purpose of program protection.
Recognize the fundamentals of T&E in support of the acquisition process.	Identify acquisition intelligence interactions from requirements through pre-Milestone A activities.
Recognize the importance of designing for sustainment and supportability planning to achieve system-readiness requirements and reduce life-cycle costs.	Recognize intelligence supportability requirements in science and technology activities.
Identify intelligence community organizations, resources and requirements that support acquisition programs.	Determine intelligence production requirements.
Recall foundational concepts related to program protection, cybersecurity, and counterintelligence as used to support an acquisition program.	Determine acquisition intelligence T&E requirements. Recognize acquisition intelligence support to sustainment activities. Recognize acquisition intelligence support to cost estimating. Determine acquisition intelligence support for acquisition and intelligence forums. Determine acquisition intelligence support for cross-program analysis across the services and at the joint level. Determine acquisition intelligence support for foreign military sales.

SOURCE: Defense Acquisition University (DAU), Training Center, Training Courses, Courses and Schedules home page.

NOTE: DAU's Courses and Schedule home webpage did not provide course objectives for CLR 101.

Together, the three DAU courses provide overviews of acquisition, requirements, and acquisition intelligence communities. ACQ 1010 and CLR 101 are recommended prerequisite courses to ACQ 110 but are not required, and AFMC's current training pipeline does not appear to require incoming civilian or military intelligence personnel to complete these courses before attending the Acquisition IFTU. Additionally, the OUSD(I) memorandum recognized "the valuable training" offered by the USAF Acquisition IFTU and accepted it in lieu of the ACQ 110 requirement before the latter became a formal training course on October 1, 2019.[19] The memorandum requires all three training courses for the foundational credential for Acquisition Intelligence; however, ACQ 110 is a much shorter course (six hours) than the acquisition IFTU (three days) and might offer fewer educational benefits than the latter.

Career Field Management: Growing Awareness and Workforce in Acquisition Intelligence

Intelligence career field managers (CFMs) have been focusing their primary efforts on the growing awareness of acquisition intelligence and its available assignments, as well as on diversifying the intelligence workforce through different hiring practices. Programs such as the Acquisition and Intelligence Experience Exchange Tour (AIEET) and Operational Experience (OPEX) are among USAF's efforts to expand awareness about acquisition intelligence among intelligence, as well as acquisition professionals. With programs such as PALACE ACQUIRE (PACQ) and Science, Mathematics, and Research for Transformation (SMART), USAF aims to diversify its Intelligence and technical (i.e., science, technology, engineering, and mathematics) workforce.

[19] DAU, Acquisition Intelligence, "First-Ever Acquisition Intelligence Course Deployed," October 8, 2019.

Growing Awareness: Career Enhancement Opportunities

Acquisition and Intelligence Experience Exchange Tour and Operational Experience Program

As noted above, USAF offers two formal career enhancement opportunities: AIEET and OPEX. AIEET is a Headquarters Air Force Personnel Center (HQ AFPC) initiative "to enhance operational awareness among Acquisition career fields and Air Force acquisition awareness among the intelligence community."[20] During AIEET, intelligence officers support product and logistics centers in helping to field systems that meet warfighters' needs, while acquisition officers gain operational perspective so that they can later apply it in their acquisition career. Officers must have a highly competitive record and return to their assigned career fields at the end of each tour.[21] The OPEX program supplements AIEET and is designed for new acquisition officer accessions to serve an operational tour in their first assignment. According to AFPC, approximately 10 percent of the scientist (61S), developmental engineer (62E), and acquisition manager (63A) AFSC accessions go through the OPEX program.[22]

The first board for AIEET occurred in 2015. Since then, eight intelligence officers were selected for the 2016–2020 AIEET. HQ AFPC's data as of May 4, 2020, provides the following information about the progress of AIEET:[23]

- Five officers have completed Intelligence Initial Skills Training and are currently in an acquisition assignment.
  - Two officers have been assigned to SMC (as PM at Space Warfighter Construct and as Project Officer for Mission Innovation at the Los Angeles AFB, California).

---

[20] myPers, "Talking Paper on Acquisition and Intelligence Experience Exchange Tour (AIEET)," myPers.af.mil account login page. Not available to the general public.

[21] Tour lengths are three years plus training: Acquisition Fundamental Course for intelligence officers and Intelligence Initial Skills Training for acquisition officers.

[22] myPers, "Talking Paper on Acquisition and Intelligence Experience Exchange Tour (AIEET)," myPers.af.mil account login page. Not available to the general public.

[23] Data provided by HQ AFPC, Intelligence Assignments.

  - Two officers have been assigned to AFLCMC (as Survivability Deputy Integrated Product Team Lead at WPAFB, Ohio, and Portfolio Lead for Modeling and Simulation at Hanscom AFB, Massachusetts).
  - One officer has been assigned to NGA (as PM for GEOINT Connectivity Services in Springfield, Virginia).
- One officer was scheduled to start the program in the summer of 2020.
- One officer has completed AIEET but has a date of separation in the summer of 2020.
- One officer has already separated from AD the USAF.

Participation in this program is limited to ten intelligence officers (and 15 acquisition officers) per year. The 2015 board will have fulfilled 60 percent of this capacity.[24] The participants in the program could go back to an acquisition organization as a senior officer (field grade officer), if the gaining billet requires a more specialized skill set.

Education with Industry

Established in 1947, sponsored by SAF/AQ, and managed by the Air Force Institute of Technology (AFIT), Education with Industry (EWI) is another career-enhancing program available to intelligence and acquisition officers, civilians, and enlisted personnel.[25] EWI is a ten-month highly selective and competitive program "designed to improve the technical, professional, and management competencies" of its participants.[26] Selected applicants embed with an industry team in one of "over 50 top-tier commercial and defense focused companies" related to their career field to learn industry best practices and develop career-specific competencies, skills, and knowledge.[27]

---

[24] Participation is also limited to 15 acquisition officers per year.

[25] Enlisted personnel are participating in EWI as part of a small beta test.

[26] AFIT, Civilian Institution Programs, "Education with Industry (EWI) Program," webpage, undated.

[27] Gloria Kwizera, "Education with Industry Program Takes JBSA Airmen on Unique Journey," 33rd Fighter Wing website, October 1, 2014; AFIT, undated.

An average of 37 students per year participated in the program between 1998 and 2018, and this number of participants has been increasing: In 2021, 77 participants are expected to complete the program; only two of them are intelligence analysts, while 18 are engineers or acquisition managers.[28] Starting on April 30, 2020, USAF officers who complete the program will also receive a special experience identifier from AFIT, which should make it easier for Air Staff, Manpower, Personnel, and Services (AF/A1) to track the military EWI fellows.[29]

Growing Workforce: Management, Hiring, Retention

Because the acquisition intelligence organization comprises both military (primarily officers) and civilian personnel, this study consulted career-field management practices for the intelligence officer and civilian corps. Intelligence officer and civilian CFMs have implemented several corps-specific measures to grow their respective workforce to make it more accessible and better prepared to support acquisition intelligence.

Military Workforce

For the civilian intelligence workforce, one such measure has been the creation of the Acquisition Intelligence Career Occupation Program discussed earlier in the "Training" section. In line with this OUSD(I) effort, HQ AF/A2, with input from AFMC, is creating an individual capability management (ICM) code that would help track and, if necessary, assign to priority billets USAF intelligence personnel with acquisition intelligence experience and training.[30] USAF currently has a special experience identifiers (SEIs) program, which helps assignment managers screen the officer database for specific experience and can be

---

[28] AFIT, "EWI History File," Maxwell Air Force Base, February 15, 2018b, provided by EWI program manager and AFIT, "Education with Industry Program Completes a Mid-Term Review," Maxwell Air Force Base, February 15, 2018a.

[29] U.S. Department of the Air Force, "Air Force Officer Classification Directory (AFOCD): The Official Guide to the Air Force Officer Classification Codes," Air Force Personnel Center, Attachment: Section III, Officer Experience Sets, April 30, 2020b, p. 14; email communication with EWI program manager on September 18, 2020.

[30] Discussion with USAF 14N career field management, August 5, 2020.

used in the officer assignment process.[31] One study found that when more officers have "specific experience/training identifiers and when more jobs identify required SEIs, it will be much easier . . . to match their experience and training to job needs."[32] Effective management of the ICM code and identification by the acquisition intelligence community of billets with specific capability requirements will be key to ensuring that jobs such as DoI at AFPEO or an intelligence focal point for a particular acquisition program can go to intelligence personnel with the requisite acquisition intelligence training and experience.

Civilian Workforce

Career field managers have been focusing on building a more diverse and inclusive civilian intelligence workforce, the majority of which (70 percent, by one estimate) has thus far consisted of retired or prior-military personnel.[33] Preference has gone to personnel with former intelligence experience and a TS security clearance with the SCI caveat. USAF has implemented the PACQ program to help diversify the intelligence civilian workforce.

The PACQ program focuses on new accessions—hiring recent college graduates from various degree programs in line with the priorities stated in the National Defense Strategy and Headquarters Air Force Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations (AF/A2/6).[34] These new hires then attend the Intelligence Initial Skills Training Course and any training or certification programs that the gaining organizations might require (e.g., ACQ 1010 for AFMC). The intelligence career field for USAF civilians does not carry a degree requirement. This makes it easier to open the career field

---

[31] U.S. Department of the Air Force, "Air Force Officer Classification Directory (AFOCD): The Official Guide to the Air Force Officer Classification Codes," Air Force Personnel Center, April 30, 2020a, p. 272.

[32] Marygail K. Brauner, Hugh G. Massey, S. Craig Moore, and Darren D. Medlin, *Improving Development and Utilization of U.S. Air Force Intelligence Officers*, Santa Monica, Calif.: RAND Corporation, TR-628-AF, 2009, p. 49.

[33] Discussion with USAF civilian career field manager, August 27, 2020; Lowell et al., 2018, p. 17.

[34] Discussion with USAF civilian career field manager, August 27, 2020.

to anyone who wants to apply. On the other hand, it makes it more difficult to hire personnel with specific technical (e.g., engineering for acquisition intelligence) education backgrounds or skills.

Intelligence civilians hired through PACQ can stay in the gaining organization, such as AFMC, for up to four years, then move on to the next vacant billet following several promotions. PACQ personnel are more likely to leave AFMC if the organization does not have a vacancy commensurate with the next promotion level for the PACQ employee. PACQ is a small program that hires between 15 and 21 intelligence civilian personnel per year to fulfill manpower requirements across all of USAF. To retain any PACQ personnel AFMC gains, AFMC needs to emphasize its demand for intelligence civilians and expand its personnel authorizations to accommodate career field growth for PACQ program personnel.

Conclusions

The number of dedicated intelligence personnel supporting the acquisition mission is relatively small (310, or 1.4 percent) when compared with the overall number of USAF government intelligence personnel (27,241). This ratio is even smaller (approximately 0.85 percent) when compared with the number of USAF government acquisition personnel (approximately 36,210).[35] These intelligence personnel are assigned across 17 different organizations within AFMC and SMC and support 14 AFPEOs with varied program portfolios that comprise 1,113 acquisition programs. The majority of intelligence personnel within AFMC are assigned to organizations supporting the various AFPEOs (AFLCMC, 21st IS, and 14th IS). Military intelligence personnel comprise 61 percent of the intelligence workforce, most of whom are officers. At the end of FY2019, approximately half of the acquisition intelligence organizations were understaffed; however, the overall net intelligence staffing at the given organizations was almost 99 percent.

Furthermore, acquisition intelligence is a technical field and requires knowledge, skills, and expertise in intelligence, engineering,

[35] U.S. Department of the Air Force, *United States Air Force Acquisition Annual Report, Fiscal Year 2018*, 2018, p. 12.

and acquisition. Relatively few individuals in USAF possess all three attributes, and even fewer are assigned to acquisition intelligence organizations. Acquisition officers are also more likely to have the stated attributes and are more likely to be found in acquisition intelligence organizations. These results are likely due to the fact that (1) the intelligence career field is not an all-technical field and does not require an ED; (2) the acquisition career field does not require an ED either, but EDs are prioritized there compared with the intelligence field; (3) priority for accessions goes to high-demand career fields (e.g., pilot) and career fields that require an ED (e.g., developmental engineer); and (4) the acquisition field provides more opportunities and with a higher participation rate than does the intelligence field for its members to broaden their experience between the two fields (e.g., AIEET, OPEX, EWI).

USAF has taken several positive steps toward improving the acquisition intelligence workforce. Acquisition intelligence organizations have established training and credential requirements and provide sufficient training in acquisition, requirements, and acquisition intelligence for their military and civilian personnel. Intelligence officers and enlisted also receive Intelligence Initial Skills Training outside the purview of acquisition intelligence, while civilians in technical fields such as engineering receive their training from undergraduate degree programs.[36] USAF has established programs to hire new accessions from various undergraduate degree programs. Finally, USAF is in the process of creating ICM codes designed to assist program owners, such as AFMC, in identifying criteria for and tracking personnel with desired capabilities.[37] The acquisition intelligence organizations have been better postured to identify requirements and receive manpower for the selected acquisition fields (e.g., S/E/A managers) than the intelligence field. These organizations have had the most success sustaining the civilian workforce in the acquisition fields. These results could be due to the following reasons: (1) enhanced recognition of requirements for acquisition positions versus intelligence positions in acquisition intelligence; (2) competing priorities to fund requirements and fill vacancies for military person-

[36] Harrington and Terry, 2016, p. 30.

[37] Email communication with 14N career field management, September 3, 2020.

nel in operational units or units directly supporting the warfighter; and (3) more attractive career development for civilian personnel in positive degree programs (e.g., engineers) versus those in nonpositive degree programs (e.g., intelligence) in acquisition intelligence.[38]

Findings and Recommendations

This chapter summarizes the specific findings of the workforce analysis and provides associated recommendations to address any personnel, training, or capability insufficiencies.

Finding: Analysis of FY2019 personnel data showed that some units were understaffed while others were overstaffed.

Recommendation: Rebalance the AFMC/SMC intelligence workforce where feasible by transferring personnel from overstaffed units to understaffed units.

Finding: The workload for intelligence personnel across acquisition intelligence organizations varies across AFPEOs. Preliminary analysis of this data and interview discussions also suggest that potential demand for intelligence support to select portfolios (e.g., AFPEO Digital, AFPEO Agile Combat Support) can, at some point, outpace the current intelligence support provided directly to these program portfolios.

Recommendation: Add personnel resources to provide more comprehensive support to more programs and meetings.

Finding: A relatively small number of USAF officers have the background in intelligence activities, engineering concepts, and acquisition processes coveted by the acquisition intelligence community. An even smaller number of these are assigned to acquisition intelligence organizations. Those intelligence officers who do have backgrounds in intelligence activities, engineering concepts, and acquisition processes

[38] Positive degree programs are those career fields that require a degree, such as engineering. In nonpositive degree programs, degrees are "highly encouraged" but not required, such as for civilians hired into the intelligence career field (0132).

in the acquisition intelligence organizations are more likely to complete their tour in acquisition intelligence and move on to other intelligence assignments. It is more likely to find acquisition officers with these same capabilities in acquisition intelligence, as these officers will remain engaged in acquisition.

Recommendation 1: Recruit more intelligence officers with engineering backgrounds.

Recommendation 2: Expand the career broadening programs (e.g., AIEET, OPEX, EWI) that allow officers, enlisted, and civilians (especially in the intelligence field) to garner all three of the stated attributes to create a consistent and sufficient workforce with this capability in acquisition intelligence (e.g., ten officers to be assigned to AFLCMC every three years).

- for USAF, encourage intelligence professionals to participate in the EWI program
- for AFMC, manage and encourage participation in AIEET (for acquisition professionals) and OPEX programs and create more opportunities for intelligence AIEET participants to support ISR-related portfolios.

Recommendation 3: Assess the existing ratios of civilian junior, midlevel, and senior intelligence personnel and expand the human capital requirement for junior billets hired through the PACQ program.

Finding: The number of S/E/A personnel is significantly larger than the number of intelligence personnel across the acquisition intelligence organizations. The S/E/A workforce is also predominantly civilian and has seen a consistent increase in its authorizations, as well as in its assignments; these trends suggest that USAF recognizes the importance of science and technology expertise for the acquisition intelligence mission. It also suggests that USAF has not had difficulty sustaining the assignments in these civilian career fields for the acquisition intelligence mission and has continued to recruit and retain these civilian professionals. This means that pairing intelligence analysts with specific engineers (e.g., experts in reverse engineering) or adding engineers to intelligence teams that provide direct support to acquisition pro-

grams could be a viable option for improving intelligence support to the acquisition mission.

Recommendation: Hire civilian technical personnel to pair with existing intelligence personnel to build intelligence support to acquisition teams, with the intent of directly supporting select acquisition programs or portfolios.[39] Further, add an Intelligence Initial Skills Training requirement to select billets.

Finding: HQ AF/A2 is creating an ICM code that would help track and, if necessary, assign to priority billets USAF intelligence personnel with the acquisition intelligence experience and training.

Recommendation 1: AFMC should determine the acquisition intelligence capability criteria to be assigned to an ICM code.

- Desiderata should include, for example, requirements for training and education, education specialty, desirable skills, and participation in career broadening programs.
- AFMC should also ensure that designated acquisition intelligence positions have complete information in position-related fields that identify education requirements, education specialty, and desirable skills to assist the AFPC assignment team with matching the right personnel to the right positions in AFMC. This can be done by, for example, matching personnel to positions providing organic intelligence support to ISR-related portfolios, senior-level or leadership positions (e.g., DoI), and advisory roles to mentor and grow the next generation of personnel with the needed capabilities.

Recommendation 2: AFPC should identify "Acquisition Intelligence" as an assignment type in intelligence officer and enlisted career reviews.

---

[39] An additional option to explore would be to develop a program of formal exchanges whereby intelligence specialists do formal rotations to acquisition programs, and vice versa. This was suggested by an early reader of the draft.

CHAPTER SIX

Conclusions and Recommendations

The threats posed by U.S. adversaries have changed, which has dramatically decreased the U.S. military's ability to operate with impunity. The air supremacy that the United States has had during two decades of counterterror combat operations in the Middle East cannot be guaranteed in a contest against a potential future peer adversary. Perhaps the perspective of air superiority is even out of reach. The threat landscape will continue changing and likely degrade further. CSAF argues that the United States needs to accelerate its improvements to meet and, to the extent possible, counter these threats or risk losing the next war. As we have suggested in this report, doing so requires continued evolutionary and new revolutionary thought and action, with a focus on addressing not only the current known threat, but also the threat as it is predicted to evolve.

Intelligence support to acquisition requires several incremental, evolutionary improvements to increase the performance and effectiveness of the ecosystem. Support to the Air Force acquisition enterprise by IC and DoD/Air Force intelligence elements has been evolving. AFMC/A2 has pressed ahead with important changes—including the MIE strategic plan and the DoI construct (which formally establishes positions within the organization that are responsible for the organization, train, and equip functions; that get a seat at the PEO tables; and that serve as intelligence SMEs to EOs). These evolutionary changes should continue, and more dramatic and long-lasting revolutionary improvements beyond the control of the AFMC/A2 are needed. These further improvements require continued Air Force leadership buy-in,

support, involvement, and advocacy for changes within and beyond the Air Force. We suggest that these evolutionary changes should be coordinated with additional revolutionary changes that are directed by Air Force leadership.

There is no single solution or set of solutions to the complex and complicated problems involved in providing intelligence support to acquisitions. Moreover, nearly every approach contains pros and cons. For example, adding additional intelligence personnel to support acquisition might improve information sharing but might not lead to positive change in terms of delivering more capable systems unless fundamental challenges such as incentive structures are changed. This suggests that resolving the root causes of many problems that the intelligence acquisition ecosystem faces will require a more holistic, whole-of-organization approach.

Long-lasting resolution requires a strategic approach to avoid islands of incremental improvement. In other words, revolutionary changes are needed for the long-term health and benefit of the enterprise. Air Force acquisition is focused on cost, schedule, and performance, as it must be, given that acquisition is constrained by the requirements and budget it is given to deliver a specified capability. Programmatic prioritization (which includes reallocating resources to some programs and away from others) is a challenge for the Air Force because of congressional restrictions, the diversity of stakeholders, and the need to support many competing missions; allocating intelligence support to acquisition reflects the same challenge.

As we have described in this report, no single entity in the Air Force acquisition enterprise (the supported organization) or the IC and the Air Force intelligence enterprise (the supporting organizations) is responsible for the overall ecosystem—not even at the level of the Secretary of Defense (who does not oversee the intelligence community, which reports up through the Director of National Intelligence). In this enterprise ecosystem, intelligence support to acquisition appears to be a lower priority for both enterprises: Acquisition efforts are focused primarily on cost, schedule, and performance, and intelligence efforts have the first priority of supporting the national intelligence mission—supporting the warfighter and policymakers.

This suggests that improvements to the intelligence support to acquisition ecosystem cannot merely be theoretical; they must match and inform the immediacy of the measurement of cost, schedule, and performance. The issue, however, is that adversary threat is a direct counter to stable program requirements. This, we suggest, is the practical hook on which intelligence could hang its support—by ensuring that requirements are actively managed throughout a system's life cycle and are informed by threat intelligence.

Information about the threat presented by intelligence personnel is inherently antagonistic to the acquisition system's quest for certainty—especially in the early stages of a program when design flexibility is at its greatest. The perception (and likely the reality) is that when received in later phases, intelligence slows program development and increases cost, triggering negative incentives when comparing programs against original baselines. How can this perception be changed not only to seek and accept intelligence but also allow program development to benefit from it through changes? *Intelligence needs to be included in acquisition in a risk-managed approach* (perhaps in a matrix with urgency on one axis and importance on the other axis). We suggest that acquisition stakeholders should think differently about roles and responsibilities and about how intelligence could improve the performance of systems under development. The desired *outcomes* of acquisition—having a capability that is able to "win"—can and should take primacy over the *outputs* of acquisition—a delivered system with certain attributes of cost, schedule, and engineering performance. This would require not only shifts within DoD (which already practices the ability to update requirements and associated cost and schedule baselines to reflect the latest intelligence on needs) but more important within Congress and its analytic arm—GAO—which measures program performance against original baselines, creating the negative incentive not to revise performance given evolving threats. Congress cannot have it both ways: wanting near-perfect cost and schedule performance, yet also demanding that defense systems be current against the evolving threats. Congress must be a partner in deciding to change requirements to meet evolving threats, and, given buy-in from all stakeholders, better mechanisms to track program outputs are needed.

Another challenge to enhancing intelligence support to acquisition is determining who will pay for the intelligence that is used to support acquisition programs. Should intelligence support be funded by the requirements owner, PM, or intelligence providers? There are reasonable arguments for and against each of these. Additionally, an associated question is what will *not* get funded, since resources are not unlimited. This gets to a deeper fundamental question on how infrastructure and support are paid for generally in DAF and wider DoD. Support such as this is "free" to the user, which causes more demand than resources allow.

Intelligence support to acquisition is not a specific "type" of intelligence. Indeed, it is one of three major roles for intelligence. As a result, the *tyranny of the urgent* that often colors intelligence support activities appears to take priority over the *20–30 years in the future intelligence support*, which is the basis for and requirement of intelligence support to acquisition.[1]

> The tyranny of the "now" is particularly keenly felt within the [intelligence] community, as a huge proportion of the available capacity is necessarily focused on current issues and short-term threats. The time and resources available to devote to horizon-scanning, indicators and warnings and maintaining the foundational intelligence that provides the critical underpinning layer from which confident intelligence assessments are derived, are therefore at a premium.[2]

The "tyranny of the now," with the focus on support to the *current* warfighter, means that the needs of the *future* warfighter are neglected. There is no easy solution to this challenge, which means that adding staff to the IC might not yield more intelligence support to acquisition, as current needs might truly be more urgent. Recommendations described earlier in this report—including ensuring an

---

[1] John Kroger, Office Life at the Pentagon Is Disconcertingly Retrograde," *Wired.com*, August 20, 2020.

[2] Sean Corbett, "The Case for Open Source Intelligence," *The Cipher Brief*, August 11, 2020.

adequate number of people within the acquisition community who have an intelligence role and the deliberate mission to pull data from and work with the formal IC—offer an approach that the acquisition community can control to increase the flows of information. Action beyond that will require senior Air Force leadership to reprioritize NASIC's missions, for example, or to advocate for a different level of support from external intelligence providers.

We have identified issues that are complex and difficult (but not impossible) to resolve. We suggest that optimal resolution requires a concerted effort across many domains, in various systems and subsystems, across two enterprises, and over an extended period. Chapters Two through Five contain topic-specific conclusions and recommendations described in more detail. Here we conclude with the key points.

- The intelligence support to the acquisition enterprise ecosystem is comprised of several entities. These entities have no single, common chain of command, and they connect via both structured (formal) and unstructured (informal) mechanisms. This connection requires support from U.S. Air Force senior leadership both to ensure change across the enterprise and to advocate for change for assets controlled outside of the Air Force. Additionally, senior leadership across all Air Force elements should continue to stress the importance of incorporating threat information into acquisition—and to make resources available for doing so. Intelligence support is not free.
- Acquisition policy and guidance do not always clarify and reinforce how and when intelligence can be continuously integrated into the acquisition process (not just at formal acquisition milestones). Emphasis is placed on cost, schedule, and performance as assigned from the requirements and budgetary communities. Thus, the requirements and budgetary community must be partners with acquisition in seeking and digesting intelligence and continually assessing and trading resources to address the biggest evolving threats. Similarly, and in accordance with institutional guidance, intelligence focuses on offering near-term (and possibly urgent) tactical and operational support and strategic

intelligence support to the warfighter and policymaker, due to their time-sensitivity, before supporting other needs, such as acquisition. Updating policy and guidance (and ensuring adequacy of resources) can help to ensure that sufficient attention is paid to acquisitions. Continually relegating intelligence support to acquisition after support to the warfighter and policymaker places the future warfighter at greater risk.

- Incentive structures are not in alignment with the goal of threat-informed acquisition, but could be improved if acquisition metrics are changed. For example, programs could be measured against updated baselines instead of original baselines, when threats are addressed midcourse. Also, programs could be measured explicitly on how well they address flexibility in the form of open systems architectures and better mechanisms to seek additional investments. Changing these metrics can change the demand signal.
- Formal methods of communicating threat and ensuring that programs are threat-informed, such as TSGs, TWGs, VOLTs, and CIPs, are useful, but do not always get the attention of busy program management. Additional intelligence support at PEOs and program offices is needed and could provide needed assistance.
- Outdated and inadequate IT infrastructure, which creates challenges and limits to information access, can be addressed with additional investments, some of which may need to be borne in acquisition program budgets. The U.S. Air Force would need to advocate for change for infrastructure controlled outside the U.S. Air Force, such as the COLISEUM, which is managed by the DIA.
- Limits on clearances within the acquisition community reduce comprehension of the true nature of the threat and thus the urgency of the response. On the intelligence side, limits on access to special access program (SAP) information by the IC create support challenges. This could be addressed by improving access availability or by seeking ways to extract less-classified insight from higher-classification documents for wider dissemination and investing in improving appropriate clearances. Lack of information on either

side of the intelligence-acquisition equation limits the objectives of both.

- The intelligence workforce supporting acquisition (the "acquisition intelligence" workforce) is likely understaffed in several areas and many analysts lack the proper skills. This can be addressed by improving hiring, training, and retention practices, and efforts are currently underway to address some of these issues (e.g., the creation of the Acquisition Intelligence Career Occupation Program Foundational Credential, the creation of an Individual Capability Management [ICM] code, and the PALACE ACQUIRE [PACQ] program). We suggest these efforts, and others like them, continue. In the end, progress is driven by people. The Air Force requires the best available.

All these recommendations would take resources and thus will require trade-offs among competing needs. In some cases, the key resources are leadership attention and reprioritization of staff attention. Adding new staff incurs bureaucratic challenges relating both to numbers of billets and paying for the people and the training. Improving IT would require direct investments. The largest cost would likely come from what it means to make effective use of better intelligence support to acquisition—namely, changing the acquisition programs themselves and thus acquiring capabilities more likely to have the desired effect against evolving threats. Knowledge of the threat is easiest to adapt to when it is received earlier in the acquisition program, when requirements are being set (before Milestone A or B), or even earlier, when technology is being researched and developed. That said, even programs farther along in the acquisition process—during engineering and manufacturing development or even production—need to remain threat-informed. If new intelligence arises that creates new operational risks for the acquired systems, acquisition management should continue to work with the requirements community to identify updates to the system or subsystems, or perhaps even more important to develop an off-ramp if the programs are no longer relevant based on the threat.

The challenge of getting resources to change the acquisition program—to allocate more money to update what is being developed by

and bought from the contractors—is beyond the scope of this project, but this is the most profound and difficult challenge, and one that trickles back through the system and creates a drag on change. But the difficulty of making these hard decisions needs to be balanced against the true threat, which is that if these are not made, then the risk of losing to adversaries in future engagement increases. DAF and wider DoD know this and invest significant efforts making these difficult decisions and trade-offs. Additional refinements in approach, policy, and investments can help, though. General Brown's message of "Accelerate Change or Lose" offers a vision for the Air Force, which can be accomplished for threat-informed acquisition with the investments we have described throughout this report.

References

Acquisition Intelligence Formal Training Unit, Wright-Patterson Air Force Base, December 2019.

AFI—*See* Air Force Instruction.

AFIT—*See* Air Force Institute of Technology.

AFLCMC—*See* Air Force Life-Cycle Management Center.

AFMC—*See* Air Force Materiel Command.

AFMAN—*See* Air Force Manual.

AFMD—*See* Air Force Mission Directive.

AFPAM—*See* Air Force Pamphlet.

AFPD—*See* Air Force Policy Directive.

Air Force Institute of Technology, Civilian Institution Programs, "Education with Industry (EWI) Program," webpage, undated. As of September 1, 2020: https://www.afit.edu/CIP/page.cfm?page=1567

———, "Education with Industry Program Completes a Mid-Term Review," Maxwell Air Force Base website, February 15, 2018a. As of September 1, 2020: https://www.maxwell.af.mil/News/Display/Article/1442963/education-with-industry-program-completes-a-mid-term-review/

———, "EWI History File," Maxwell Air Force Base, February 15, 2018b.

Air Force Instruction 10-601, *Operational Capability Requirements Development*, U.S. Department of the Air Force, November 6, 2013.

Air Force Instruction 14-111, *Intelligence Support to the Acquisition Life Cycle*, U.S. Department of the Air Force, Incorporating Change 1, June 16, 2014.

Air Force Instruction 63-101/20-101, *Integrated Life-Cycle Management*, U.S. Department of the Air Force, May 9, 2017.

Air Force Life-Cycle Management Center, *Standard Process for Intelligence Sensitivity Determination*, Version 3.2, April 19, 2018.

———, *Standard Process for Intelligence Supportability Analysis*, Version 2.0, September 19, 2019.

Air Force Manual 14-401, *Intelligence Analysis and Targeting Tradecraft/Data Standard*, U.S. Department of the Air Force, August 8, 2019.

Air Force Materiel Command, "AFMC's Materiel Intelligence Enterprise Strategic Approach," pamphlet, undated.

———, "Air Force Material Command," Factsheet webpage, June 22, 2020. As of March 8, 2021:
https://www.afmc.af.mil/About-Us/Fact-Sheets/Display/Article/2229053/air-force-materiel-command/

Air Force Mission Directive 24, *National Air and Space Intelligence Center (NASIC)*, U.S. Department of the Air Force, September 22, 2016.

Air Force Pamphlet 63-113, *Program Protection Planning for Life-Cycle Management*, U.S. Department of the Air Force, October 17, 2013.

Air Force Policy Directive 10-6, *Capability Requirements Development*, U.S. Department of the Air Force, November 6, 2013.

Allport, Gordon W., and Leo Postman, *The Psychology of Rumor*, Henry Holt, 1947.

Baron, Robert A., and Jerald Greenberg, *Behavior in Organizations: Understanding and Managing the Human Side of Work (Vol. 1)*, Allyn & Bacon, 1990.

Ben-Menahem, Shiko M., Georg Von Krogh, Zeynep Erden, and Andreas Schneider, "Coordinating Knowledge Creation in Multidisciplinary Teams: Evidence from Early-Stage Drug Discovery," *Academy of Management Journal*, Vol. 59, No. 4, 2016.

Bertuca, Tony, "Pentagon Finds China Outpacing U.S. in Shipbuilding and Missile Tech," *Inside Defense*, September 1, 2020.

Bliss, Gary, "Seamless Threat Awareness in Acquisition Programs," presentation slides, U.S. Department of Defense, August 20, 2015. As of March 8, 2021:
https://www.ndia.org/-/media/sites/ndia/divisions/ipmd/2015-08-meeting/3_bliss_improving_intel_sa_17aug15_ses.ashx?la=en

Brauner, Marygail K., Hugh G. Massey, S. Craig Moore, and Darren D. Medlin, *Improving Development and Utilization of U.S. Air Force Intelligence Officers*, Santa Monica, Calif.: RAND Corporation, TR-628-AF, 2009. As of March 8, 2021:
https://www.rand.org/pubs/technical_reports/TR628.html

Brody, R., "Gossip: Pros and Cons," *USAIR Magazine*, November 1989.

Brown, Charles Q., Jr., "Accelerate Change or Lose," *Air Force Magazine*, August 2020. As of March 22, 2021: https://www.airforcemag.com/app/uploads/2020/08/CSAF-22-Strategic-Approach-Accelerate-Change-or-Lose-31-Aug-2020.pdf

Bunch, Arnold W., Jr., *AFMC Strategic Plan*, July 2020. As of March 22, 2021: https://www.afmc.af.mil/Portals/13/Final%20Strat%20Plan_signed_crp%2013%20Jul%2020.pdf

Burt, Ronald S., *Structural Holes: The Social Structure of Competition*, Harvard University Press, Cambridge, 1992.

Chairman of the Joint Chiefs of Staff Instruction J8, *Manual for the Operation of the Joint Capabilities Integration and Development System*, August 31, 2018.

Chairman of the Joint Chiefs of Staff Instruction 3317.01, *Intelligence Oversight Responsibilities, Procedures, and Oversight Functions*, January 6, 2020.

Chairman of the Joint Chiefs of Staff Instruction 5123.01H, *Charter of the Joint Requirements Oversight (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)*, August 31, 2018.

Corbett, Sean, "The Case for Open Source Intelligence," *The Cipher Brief*, August 11, 2020. As of April 14, 2021: https://www.thecipherbrief.com/column_article/the-case-for-open-source-intelligence

Crampton, S. M., J. W. Hodge, and J. M. Mishra, "The Informal Communication Network: Factors Influencing Grapevine Activity," *Public Personnel Management*, Vol. 27, No. 4, 1998, pp. 569–584.

Cross, Rob, and Laurence Prusak, "The People Who Make Organizations Go—or Stop," *Harvard Business Review*, Vol. 80, 2002.

Cross, Rob, and Robert Thomas, "A Smarter Way to Network," *Harvard Business Review*, Vol. 89, 2011.

DAU—*See* Defense Acquisition University.

Davis, Keith, "Management Communication and the Grapevine," *Harvard Business Review*, Vol. 31, 1953.

———, "The Care and Cultivation of the Corporate Grapevine," *Dun's Management Review*, Vol. 62, 1973.

Defense Acquisition University, "Adaptive Acquisition Framework Pathways," webpage, undated(a). As of March 22, 2021: https://aaf.dau.edu/aaf/aaf-pathways/

———, "Milestone Document Identification: The DoD Information and Reporting Requirements Tool," undated(b). As of December 7, 2020: https://www.dau.edu/mdid/Pages/Default.aspx

———, *Defense Acquisition Guidebook*, Fort Belvoir, Va.: Defense Acquisition University, August 17, 2019. As of March 22, 2021: www.dau.edu/tools/dag

———, Acquisition Intelligence, "First-Ever Acquisition Intelligence Course Deployed," October 8, 2019. As of August 31, 2020: https://www.dau.edu/training/career-development/acq-intel/blog/First-Ever-Acquisition-Intelligence-Course-Deployed

———, Training Center, Training Courses, Courses and Schedules home page, "CLR 101 Introduction to the Joint Capabilities Integration & Development System," October 16, 2019a. As of August 31, 2020: https://icatalog.dau.edu/onlinecatalog/courses.aspx?crs_id=1890

———, Training Center, Training Courses, Courses and Schedules home page, "ACQ 110 Fundamentals of Acquisition Intelligence," October 30, 2019b. As of March 22, 2021: https://icatalog.dau.edu/onlinecatalog/courses.aspx?crs_id=12318

———, Training Center, Training Courses, Courses and Schedules home page, "ACQ 1010 Fundamentals of Systems Acquisition Management," May 19, 2020. As of August 31, 2020: https://icatalog.dau.edu/onlinecatalog/courses.aspx?crs_id=12339

Defense Intelligence Agency Instruction 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, February 1, 2013.

Department of Defense Directive 3000.06, *Combat Support Agencies (CSAs)*, Washington, D.C.: U.S. Department of Defense, June 27, 2013.

Department of Defense Directive 5000.01, *The Defense Acquisition System*, Washington, D.C.: U.S. Department of Defense, September 9, 2020.

Department of Defense Directive 5105.21, *Defense Intelligence Agency*, Washington, D.C.: U.S. Department of Defense, March 18, 2008.

Department of Defense Directive 5200.47E, *Anti-Tamper (AT)*, Washington, D.C.: U.S. Department of Defense, September 4, 2015, Incorporating Change 2, August 31, 2018.

Department of Defense Directive 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*, Washington, D.C.: U.S. Department of Defense, January 22, 2013, Incorporating Change 1, August 29, 2017.

Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015.

Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, May 12, 2003, Incorporating Change 2, August 31, 2018.

Department of Defense Instruction 5000.02, *Operation of the Adaptive Acquisition Framework*, Washington, D.C., U.S. Department of Defense, January 23, 2020.

Department of Defense Instruction 5000.02T, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015, Incorporating Change 3, August 10, 2017.

Department of Defense Instruction 5000.02T, *Operation of the Defense Acquisition System*, Washington, D.C., U.S. Department of Defense, January 7, 2015, Incorporating Change 9, November 19, 2020.

Department of Defense Instruction 5000.75, *Business Systems Requirements and Acquisition*, Washington, D.C., U.S. Department of Defense, February 2, 2017.

Department of Defense Instruction 5000.80, *Operation of the Middle Tier of Acquisition (MTA)*, Washington, D.C., U.S. Department of Defense, December 30, 2019.

Department of Defense Instruction 5000.85, *Major Capability Acquisition*, Washington, D.C., U.S. Department of Defense, August 6, 2020.

Department of Defense Instruction 5000.86, *Acquisition Intelligence*, Washington, D.C., U.S. Department of Defense, September 11, 2020.

Department of Defense Instruction 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, Washington, D.C., U.S. Department of Defense, May 28, 2017, Incorporating Change 1, November 17, 2017.

Department of Defense Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, Washington, D.C., U.S. Department of Defense, November 5, 2012, Incorporating Change 2, July 27, 2017.

Department of Defense Instruction 8500.01, *Cybersecurity*, Washington, D.C., U.S. Department of Defense, March 14, 2014, Incorporating Change 1, October 7, 2019.

Department of Defense Instruction O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, Washington, D.C., U.S. Department of Defense, June 8, 2011, Incorporating Change 1, October 15, 2013. Not available to the general public.

Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, Washington, D.C., U.S. Department of Defense, August 8, 2016.

DIAI—*See* Defense Intelligence Agency Instruction.

DOD—*See* U.S. Department of Defense.

DoDD—*See* Department of Defense Directive.

DoDI—*See* Department of Defense Instruction.

DoDM—*See* Department of Defense Manual.

Edem, Tim, "AFMC Intelligence Squadron: Acquisition Intelligence Cost Estimating," SCEA-ISPA Joint Annual Conference and Training Workshop, 2008. As of September 21, 2020: http://www.iceaaonline.com/ready/wp-content/uploads/2017/09/LL07.pdf

Email correspondence with Headquarters Air Force Materiel Command, Intelligence Directorate, Intelligence, Surveillance, and Reconnaissance Forces Division, Workforce Development.

FAR—*See* Federal Acquisition Regulation.

Federal Acquisition Regulation, Part 6 - Competition Requirements, Subpart 6.3 - Other Than Full and Open Competition, 6.301 - Policy, March 10, 2021.

Federal Acquisition Regulation, Part 16 - Types of Contracts, Subpart 16.2 - Fixed-Price Contracts, 16.201 - General, March 10, 2021.

Ganswein, Wolfgang, *Effectiveness of Information Use for Strategic Decision-Making*, Gabler, 2011.

GAO—*See* U.S. Government Accountability Office.

Garamone, Jim, "Mattis: 2018 Budget Will Continue Readiness Recovery," U.S. Army, June 15, 2017. As of March 8, 2021: https://www.army.mil/article/189422/mattis_2018_budget_will_continue_readiness_recovery

Gargiulo, Martin, Gokhan Ertug, and Charles Galunic, "The Two Faces of Control: Network Closure and Individual Performance among Knowledge Workers," *Administrative Science Quarterly*, Vol. 54, No. 2, 2009, pp. 299–333.

Hargadon, Andrew, and Robert I. Sutton, "Technology Brokering and Innovation in a Product Development Firm," *Administrative Science Quarterly*, Vol. 42, No. 4, 1997, pp. 716–749.

Harrington, Lisa M., and Tara L. Terry, *Air Force Officer Accession Planning*, Santa Monica, Calif.: RAND Corporation, RR-1099-AF, 2016. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RR1099.html

Hura, Myron, and Gary McLeod, *Ensuring Adequate Intelligence Support for the Acquisition of New Weapon Systems*, Santa Monica, Calif.: RAND Corporation, DB-125-CMS, 1995. As of March 8, 2021: https://www.rand.org/pubs/documented_briefings/DB125.html

Jian, Guowei, "Informal Communication and the Grapevine," in *Encyclopedia of Management Theory*, 2013.

Krackhardt, David, and Jeffrey R. Hanson, "Informal Networks: The Company Behind the Charts," *Harvard Business Review*, Vol. 71, 1993.

Kroger, John, "Office Life at the Pentagon Is Disconcertingly Retrograde," *Wired.com*, August 20, 2020. As of March 22, 2021: https://www.wired.com/story/opinion-office-life-at-the-pentagon-is-disconcertingly-retrograde/

Kwizera, Gloria "Education with Industry Program Takes JBSA Airmen on Unique Journey," 33rd Fighter Wing website, October 1, 2014. As of September 1, 2020: https://www.33fw.af.mil/News/Features/Display/Article/877560/education-with-industry-program-takes-jbsa-airmen-on-unique-journey/

Lowell, P., Tiki Mitchell, Marc Luoma, and Vivian Cocca, *Military Department and Service Acquisition Intelligence Workforce*, Institute for Defense Analyses Project 4468, August 21, 2018.

McDermott, Richard, and Douglas Archibald, "Harnessing Your Staff's Informal Networks," *Harvard Business Review*, Vol. 88, 2010.

McKernan, Megan, Jeffrey A. Drezner, and Jerry M. Sollinger, *Tailoring the Acquisition Process in the U.S. Department of Defense*, Santa Monica, Calif.: RAND Corporation, RR-966-OSD, 2015. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RR966.html

Military Personnel Database System data from Fiscal Years 2010 to 2019.

myPers, "Talking Paper on Acquisition and Intelligence Experience Exchange Tour (AIEET)," myPers.af.mil account login page. Not available to the general public.

Niedergassel, Benjamin, *Knowledge Sharing in Research Collaborations*, Springer Science and Business Media, 2011.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Implementation Directive for Better Buying Power 3.0—Achieving Dominant Capabilities Through Technical Excellence and Innovation," Washington, D.C.: U.S. Department of Defense, April 9, 2015a. As of March 24, 2021: https://www.acq.osd.mil/fo/docs/betterBuyingPower3.0(9Apr15).pdf

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Report to Congress on Performance Assessments and Root Cause Analyses," Washington, D.C.: U.S. Department of Defense, 2015b. As of March 22, 2021: https://www.acq.osd.mil/aap/assets/docs/2015-parca-report-to-congress.pdf

Personnel Accountability System data, March 2020.

Public Law 114-92, National Defense Authorization Act of Fiscal Year 2016, Section 804.

Raz, Ornit, and Peter A. Gloor, "Size Really Matters—New Insights for Start-Ups' Survival," *Management Science*, Vol. 53, No. 2, 2007, pp. 169–177.

Reagans, Ray, and Bill McEvily, "Network Structure and Knowledge Transfer: The Effects of Cohesion and Range," *Administrative Science Quarterly*, Vol. 48, No. 2, 2003, pp. 240–267.

Rich, Benjamin, and Leo Janos, *Skunk Works: A Personal Memoir of My Years at Lockheed*, New York: Little Brown, 1996.

Rollins, Amy, "AFMC Intelligence Squadron Redesignated as 21st Intelligence Squadron," *Wright-Patterson AFB News*, October 26, 2012. As of September 21, 2020:
https://web.archive.org/web/20140109000346/http://www.wpafb.af.mil/news/story.asp?id=123323833

Schneider, Grant. *DS Strategic Vision 2012–2017*, Washington, D.C.: Defense Intelligence Agency, 2012.

Secretary of the Air Force for Acquisition Integration, Air Force acquisition programs listing, Monthly Acquisition Report, November 2019.

Sheehan, Neil, *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon*, New York: Vintage, 2009.

Sutton, H., and L. W. Porter, "A Study of the Grapevine in a Governmental Organization," *Personnel Psychology*, Vol. 21, 1968, pp. 223–230.

U.S. Code, Title 10, Section 137, Under Secretary of Defense for Intelligence and Security, December 20, 2019.

U.S. Code, Title 10, Section 181(d)(1)(B), Joint Requirements Oversight Council, December 20, 2019.

U.S. Code, Title 10, Section 2303a, Development of Deployable Systems to Include Consideration of Force Protection in Asymmetric Threat Environments, January 24, 2020.

U.S. Code, Title 10, Section 2430(a)(2)(A), Major Defense Acquisition Program Defined, January 24, 2020.

U.S. Code, Title 10, Section 2433a, Critical Cost Growth in Major Defense Acquisition Programs, January 24, 2020.

U.S. Department of the Air Force, "Air Force Office of Special Investigations: Fact Sheet," April 15, 2005. As of March 22, 2021:
https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104502/air-force-office-of-special-investigations/

———, "Air Force Doctrine Publication 2-0 - Global Integrated ISR Operations," January 29, 2015. As of April 13, 2021:
https://www.doctrine.af.mil/Doctrine-Publications/AFDP-2-0-Global-Integrated-ISR-Ops/

———, *United States Air Force Acquisition Annual Report, Fiscal Year 2018*, 2018. As of September 2, 2020:
https://www.af.mil/Portals/1/documents/5/FY18_AQReport.pdf

———, *Air Force Guidance Memorandum for Rapid Acquisition Activities*, 63-01, June 27, 2019a.

———, *AF/A5R Requirements Development Guidebook, Volume 1: Guidelines, Oversight and Governance*, Air Force Requirements Integration Division, Washington, D.C., December 5, 2019b.

———, "Air Force Officer Classification Directory (AFOCD): The Official Guide to the Air Force Officer Classification Codes," April 30, 2020a.

———, "Air Force Officer Classification Directory (AFOCD): The Official Guide to the Air Force Officer Classification Codes," Attachment: Section III, Officer Experience Sets, April 30, 2020b.

U.S. Department of Defense, "Program Protection Plan Outline and Guidance, Version 1.0," Washington, D.C., Deputy Assistant Secretary of Defense Systems Engineering, July 2011.

———, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018a.

———, "Middle Tier of Acquisition (Rapid Prototyping/Rapid Fielding) Interim Authority and Guidance," Washington, D.C., Under Secretary of Defense for Acquisition and Sustainment, April 16, 2018b.

———, "Acquisition Intelligence Career Occupation Program Foundational Credential," Memorandum, Washington, D.C.: Office of the Under Secretary of Defense, July 30, 2019.

U.S. Government Accountability Office, *Defense Intelligence: Additional Steps Could Better Integrate Intelligence Input into DoD's Acquisition of Major Weapon Systems*, Washington, D.C., GAO-17-10, November 2016.

———, *Missile Defense: Further Collaboration with the Intelligence Community Would Help MDA Keep Pace with Emerging Threats*, Washington, D.C., GAO-20-177, December 2019.

Uzzi, Brian, "Embeddedness in the Making of Financial Capital: How Social Relations and Networks Benefit Firms Seeking Financing," *American Sociological Review*, Vol. 64, No. 4, 1999, pp. 481–505.

Willis, Patrick, "Joint Capabilities Integration and Development System (JCIDS): A Primer," Fort Belvoir, Va.: Defense Acquisition University, January 31, 2019.

PROJECT AIR FORCE

Asked by the Air Force Materiel Command to determine whether the efficacy of existing and future acquisition programs and strategies could be improved, RAND's Project AIR FORCE engaged a team of experts to analyze U.S. Air Force intelligence support to the acquisition community. The main challenge they found is in ensuring the ability of the acquisition community to deliver capabilities that meet a threat as it exists when capabilities are delivered, not as it was when requirements were set. Doing so requires understanding the distinct cultures, resource constraints and incentives, and goals of the acquisition and intelligence enterprises themselves, all of which have been shaped during decades when the U.S. military dominated and its weaponry had no peer.

Thus, the authors provide an overview of the acquisition enterprise ecosystem, which includes the Department of Defense and the Intelligence Community, as well as Congress and other stakeholders. Focusing on interactions between acquisition and intelligence processes and personnel, including current disincentives to interacting, and taking into account resource constraints, they point to ways to enhance information sharing and workforce development in order to ensure that U.S. Air Force acquisition is adequately informed by intelligence in an environment of increasingly sophisticated threats from peer and near-peer adversaries.

$31.00

ISBN-10 1-9774-0814-1
ISBN-13 978-1-9774-0814-3

www.rand.org

RR-A537-1